PCT/JP2004/002228

日本国特許庁
JAPAN PATENT OFFICE

25.2.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

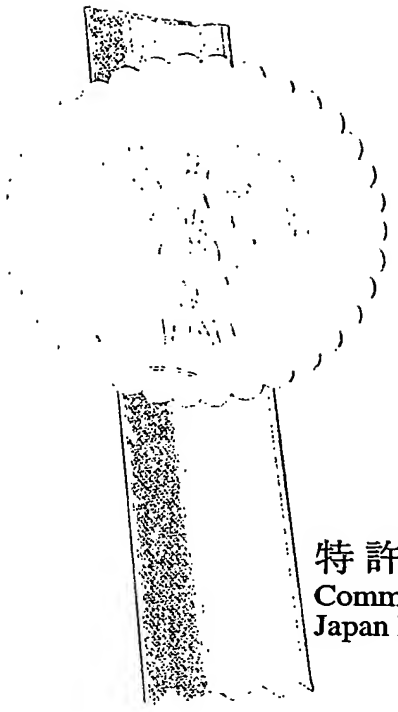
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　９月　４日

出願番号
Application Number: 特願２００３－３１２１５６

[ST. 10/C]: [ＪＰ２００３－３１２１５６]

出願人
Applicant(s): 学校法人同志社
株式会社国際電気通信基礎技術研究所



２００４年　３月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０２５１００

【書類名】　特許願
【整理番号】　1031243
【提出日】　平成15年 9月 4日
【あて先】　特許庁長官殿
【国際特許分類】　H04B 13/00
【発明者】
　【住所又は居所】　京都府京田辺市多々羅都谷１－３　同志社大学内
　【氏名】　笹岡　秀一
【発明者】
　【住所又は居所】　京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内
　【氏名】　青野　智之
【発明者】
　【住所又は居所】　京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内
　【氏名】　大平　孝
【特許出願人】
　【識別番号】　503027931
　【住所又は居所】　京都府京都市上京区今出川通烏丸東入玄武町６０１番地
　【氏名又は名称】　学校法人同志社
【特許出願人】
　【識別番号】　393031586
　【住所又は居所】　京都府相楽郡精華町光台二丁目２番地２
　【氏名又は名称】　株式会社国際電気通信基礎技術研究所
【代理人】
　【識別番号】　100064746
　【弁理士】
　【氏名又は名称】　深見　久郎
【選任した代理人】
　【識別番号】　100085132
　【弁理士】
　【氏名又は名称】　森田　俊雄
【選任した代理人】
　【識別番号】　100083703
　【弁理士】
　【氏名又は名称】　仲村　義平
【選任した代理人】
　【識別番号】　100096781
　【弁理士】
　【氏名又は名称】　堀井　豊
【選任した代理人】
　【識別番号】　100098316
　【弁理士】
　【氏名又は名称】　野田　久登
【選任した代理人】
　【識別番号】　100109162
　【弁理士】
　【氏名又は名称】　酒井　將行
【国等の委託研究の成果に係る記載事項】　平成１５年度通信・放送機構、研究テーマ「自律分散型無線ネットワークの研究開発」に関する委託研究、産

業活力再生特別措置法第３０条の適用を受ける特許出願

【手数料の表示】
　【予納台帳番号】　008693
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
指向性を電気的に切換え可能な第１のアンテナと、
第２のアンテナと、
前記第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する第１及び第２の無線装置とを備え、
前記第１の無線装置は、前記第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第２の無線装置から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成し、
前記第２の無線装置は、前記第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第１の無線装置から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて前記第１の秘密鍵と同じ第２の秘密鍵を生成する、無線通信システム。
【請求項２】
前記第１及び第２の受信信号プロファイルの各々は、前記複数個の指向性に対応した複数の強度からなり、
前記第１及び第２の無線装置は、前記複数の強度を多値化してそれぞれ前記第１及び第２の秘密鍵を生成する、請求項１に記載の無線通信システム。
【請求項３】
前記第１及び第２の無線装置は、時分割復信方式により前記複数の電波を送受信する、請求項１または請求項２に記載の無線通信システム。
【請求項４】
前記第１の無線装置は、前記生成した第１の秘密鍵が前記第２の秘密鍵に一致することを確認する、請求項１から請求項３のいずれか１項に記載の無線通信システム。
【請求項５】
前記第１の無線装置は、前記生成した第１の秘密鍵が前記第２の秘密鍵に不一致であるとき、前記第１の秘密鍵を前記第２の秘密鍵に一致させる、請求項１から請求項３のいずれか１項に記載の無線通信システム。
【請求項６】
前記第１のアンテナは、盗聴者の端末に近接して配置された第１の無線装置に設置される、請求項１から請求項５のいずれか１項に記載の無線通信システム。
【請求項７】
前記第１及び第２の無線装置は、前記第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する、請求項１から請求項６のいずれか１項に記載の無線通信システム。

【書類名】明細書
【発明の名称】無線通信システム
【技術分野】
【０００１】
この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システムに関するものである。
【背景技術】
【０００２】
最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来から情報を暗号化して送信することが行なわれている。
【０００３】
情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性が高いが、大容量のデータの暗号化には向かない。
【０００４】
一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。
【０００５】
そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、２つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（非特許文献１）。
【０００６】
この方法は、２つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて生成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。
【０００７】
このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを２つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。
【非特許文献１】堀池　元樹、笹岡　秀一，「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」，信学技報，社団法人　電子情報通信学会，２００２年１０月，TECHNICAL REPORT OF IEICE RCS2002-173，ｐ．７－１２
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかし、２つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。
【０００９】
そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、秘密鍵の盗聴を抑制可能な無線通信システムを提供することである。
【課題を解決するための手段】
【００１０】
この発明によれば、無線通信システムは、第１及び第２のアンテナと、第１及び第２の無線装置とを備える。第１のアンテナは、指向性を電気的に切換え可能である。第１及び

第２の無線装置は、第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第１の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第２の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成する。また、第２の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第１の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて第１の秘密鍵と同じ第２の秘密鍵を生成する。

【００１１】

好ましくは、第１及び第２の受信信号プロファイルの各々は、複数個の指向性に対応した複数の強度からなる。第１及び第２の無線装置は、複数の強度を多値化してそれぞれ第１及び第２の秘密鍵を生成する。

【００１２】

好ましくは、第１及び第２の無線装置は、時分割復信方式により複数の電波を送受信する。

【００１３】

好ましくは、第１の無線装置は、生成した第１の秘密鍵が第２の秘密鍵に一致することを確認する。

【００１４】

好ましくは、第１の無線装置は、生成した第１の秘密鍵が第２の秘密鍵に不一致であるとき、第１の秘密鍵を第２の秘密鍵に一致させる。

【００１５】

好ましくは、第１のアンテナは、盗聴者の端末に近接して配置された第１の無線装置に設置される。

【００１６】

好ましくは、第１及び第２の無線装置は、第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

【発明の効果】

【００１７】

この発明による無線通信システムにおいては、指向性を電気的に切換え可能な第１のアンテナを介して２つの無線装置間で所定のデータが送受信される。そして、第１のアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが２つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて２つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、２つの無線装置間に形成される伝送路に固有である。即ち、２つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、２つの端末装置で生成される受信信号プロファイルと異なる。

【００１８】

従って、この発明によれば、２つの無線装置において作成される秘密鍵の盗聴を抑制できる。

【発明を実施するための最良の形態】

【００１９】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２０】

図１は、この発明の実施の形態による無線通信システムの概略図である。無線通信システム１００は、無線装置１０，３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０は、例えば、ユーザの移動体通信端末である。また、無線装置３０は、例

えば、無線アクセスポイントである。

【００２１】

アンテナ１１は、無線装置１０に装着される。そして、アンテナ１１は、全方位性のアンテナである。アレーアンテナ２０は、アンテナ素子２１～２７を備える。アンテナ素子２４は、給電素子であり、アンテナ素子２１～２３，２５～２７は、無給電素子である。そして、アンテナ素子２４は、アンテナ素子２１～２３，２５～２７によって取り囲まれている。無給電素子であるアンテナ素子２１～２３，２５～２７に装荷された可変容量素子であるバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ２０は、適応ビーム形成が可能である。

【００２２】

即ち、アレーアンテナ２０は、無線装置３０に含まれるバラクタダイオード（図示せず）に印加する直流電圧を変えることによって指向性が変えられる。従って、アレーアンテナ２０は、電気的に指向性を切換え可能なアンテナである。そして、アレーアンテナ２０は、無線装置３０に装着される。

【００２３】

無線装置１０と無線装置３０との間で通信が行われる場合、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による影響を受けて伝搬する。中間物４０としては、反射物及び障害物が想定される。中間物４０が反射物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって反射されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。また、中間物４０が障害物である場合、無線装置１０のアンテナ１１または無線措置３０のアレーアンテナ２０から出射した電波は、中間物４０によって回折されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。

【００２４】

このように、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による反射を受けて反射波として伝搬したり、中間物４０による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬した電波がどのような成分により構成されるかによって無線装置１０と無線装置３０との間の伝送路の特性が決定される。

【００２５】

この発明においては、無線装置１０と無線装置３０との間で通信が行なわれる場合、アレーアンテナ２０の指向性を複数個に変えて時分割復信（ＴＤＤ：Ｔｉｍｅ　Ｄｉｖｉｓｉｏｎ　Ｄｕｐｌｅｘ）により所定のデータが同一の周波数で無線装置１０，３０間で送受信される。そして、無線装置１０，３０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルＲＳＳＩを生成し、その生成した受信信号プロファイルＲＳＳＩに基づいて秘密鍵を作成する。

【００２６】

秘密鍵が無線装置１０，３０において生成されると、無線装置１０，３０は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

【００２７】

図２は、図１に示す一方の無線装置１０の概略ブロック図である。無線装置１０は、信号発生部１１０と、送信処理部１２０と、アンテナ部１３０と、受信処理部１４０と、プロファイル生成部１５０と、鍵作成部１６０と、鍵一致確認部１７０と、鍵記憶部１８０と、鍵一致化部１９０と、暗号部２００と、復号部２１０とを含む。

【００２８】
信号発生部１１０は、秘密鍵を生成するときに無線装置３０へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部１２０へ出力する。送信処理部１２０は、変調、周波数変換、多元接続及び送信信号の増幅等の送信系の処理を行なう。アンテナ部１３０は、図１に示すアンテナ１１からなり、送信処理部１２０からの信号を無線装置３０へ送信し、無線装置３０からの信号を受信して受信処理部１４０またはプロファイル生成部１５０へ供給する。
【００２９】
受信処理部１４０は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部１４０は、受信処理を行なった信号を必要に応じて鍵一致確認部１７０、鍵一致化部１９０及び復号部２１０へ出力する。
【００３０】
プロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部１３０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。
【００３１】
鍵作成部１６０は、プロファイル生成部１５０からの受信信号プロファイルＲＳＳＩに基づいて秘密鍵Ｋｓ１を作成する。そして、鍵作成部１６０は、作成した秘密鍵Ｋｓ１を鍵一致確認部１７０及び鍵一致化部１９０へ出力する。
【００３２】
鍵一致確認部１７０は、所定の信号を送信処理部１２０、アンテナ部１３０及び受信処理部１４０を介して無線装置３０と送受信し、鍵作成部１６０によって作成された秘密鍵Ｋｓ１が無線装置３０において作成された秘密鍵Ｋｓ２に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致すると確認したとき、秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。また、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に不一致であることを確認したとき、不一致信号ＮＭＴＨを生成して鍵一致化部１９０へ出力する。
【００３３】
鍵記憶部１８０は、鍵一致確認部１７０及び鍵一致化部１９０からの秘密鍵Ｋｓ１を記憶する。また、鍵記憶部１８０は、記憶した秘密鍵Ｋｓ１を暗号部２００及び復号部２１０へ出力する。なお、鍵記憶部１８０は、秘密鍵Ｋｓ１を一時的、例えば、無線装置３０との通信の間だけ記憶するようにしてもよい。
【００３４】
鍵一致化部１９０は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受けると、後述する方法によって秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる。そして、鍵一致化部１９０は、一致させた秘密鍵が秘密鍵Ｋｓ２に一致することを鍵一致確認部１７０における方法と同じ方法によって確認する。
【００３５】
暗号部２００は、送信データを鍵記憶部１８０に記憶された秘密鍵Ｋｓ１によって暗号して送信処理部１２０へ出力する。復号部２１０は、受信処理部１４０からの信号を鍵記憶部１８０からの秘密鍵Ｋｓ１によって復号して受信データを生成する。
【００３６】
図３は、図１に示す他方の無線装置３０の概略ブロック図である。無線装置３０は、無線装置１０のアンテナ部１３０をアンテナ部２２０に代え、指向性設定部２３０を追加したものであり、その他は、無線装置１０と同じである。
【００３７】
アンテナ部２２０は、図１に示すアレーアンテナ２０からなる。そして、アンテナ部２２０は、送信処理部１２０からの信号を指向性設定部２３０によって設定された指向性で無線装置１０へ送信し、無線装置１０からの信号を指向性設定部２３０によって設定され

た指向性で受信して受信処理部１４０またはプロファイル生成部１５０へ出力する。

【００３８】

指向性設定部２３０は、アンテナ部２２０の指向性を設定する。また、指向性設定部２３０は、無線装置１０，３０において秘密鍵Ｋｓ１，Ｋｓ２を生成するとき、後述する方法により所定の順序に従ってアンテナ部２２０の指向性を順次切換える。

【００３９】

なお、無線装置３０のプロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部２２０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。

【００４０】

図４は、図３に示す指向性設定部２３０の概略ブロック図である。指向性設定部２３０は、制御電圧発生回路２３１と、バラクタダイオード２３２とを含む。制御電圧発生回路２３１は、制御電圧ＣＬＶ１～ＣＬＶｎ（ｎは自然数）を順次発生し、その発生した制御電圧ＣＬＶ１～ＣＬＶｎをバラクタダイオード２３２へ順次出力する。バラクタダイオード２３２は、制御電圧ＣＬＶ１～ＣＬＶｎに応じて無給電素子であるアンテナ素子２１～２３，２５～２７に装荷される容量を変え、アレーアンテナ２０の指向性を複数個に順次変える。

【００４１】

図５は、図２及び図３に示す鍵一致確認部１７０の概略ブロック図である。鍵一致確認部１７０は、データ発生部１７１と、データ比較部１７２と、結果処理部１７３とを含む。なお、無線装置１０，３０の鍵一致確認部１７０は、同じ構成からなるが、図５においては、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認する動作を説明するために、無線装置３０においてはデータ発生部１７１のみを示す。

【００４２】

データ発生部１７１は、鍵作成部１６０から秘密鍵Ｋｓ１を受けると、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認するための鍵確認用データＤＣＦＭ１を発生し、その発生した鍵確認用データＤＣＦＭ１を送信処理部１２０及びデータ比較部１７２へ出力する。

【００４３】

この場合、データ発生部１７１は、秘密鍵Ｋｓ１から非可逆的な演算及び一方向的な演算等により、鍵確認用データＤＣＦＭ１を発生する。より具体的には、データ発生部１７１は、秘密鍵Ｋｓ１またはＫｓ２のハッシュ値を演算することにより、鍵確認用データＤＣＦＭ１を発生する。

【００４４】

データ比較部１７２は、データ発生部１７１から鍵確認用データＤＣＦＭ１を受け、無線装置３０のデータ発生部１７１で発生された鍵確認用データＤＣＦＭ２を受信処理部１４０から受ける。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１を鍵確認用データＤＣＦＭ２と比較する。データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致するとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。

【００４５】

また、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１７２は、不一致信号ＮＭＴＨを鍵一致化部１９０へ出力し、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００４６】

結果処理部１７３は、データ比較部１７２から一致信号ＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１を鍵記憶部１８０へ記憶する。

【００４７】

図６は、図２及び図３に示す鍵一致化部１９０の概略ブロック図である。鍵一致化部１９０は、擬似シンドローム作成部１９１と、不一致ビット検出部１９２と、鍵不一致訂正部１９３と、データ発生部１９４と、データ比較部１９５と、結果処理部１９６とを含む。

【００４８】

なお、無線装置１０，３０の鍵一致化部１９０は、同じ構成からなるが、図６においては、秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる動作を説明するために、無線装置３０においては擬似シンドローム作成部１９１のみを示す。

【００４９】

擬似シンドローム作成部１９１は、鍵一致確認部１７０のデータ比較部１７２から不一致信号ＮＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１のシンドロームx_1を演算する。より具体的には、擬似シンドローム作成部１９１は、秘密鍵Ｋｓ１のビットパターンx_1を検出し、ビットパターンx_1に対して検査行列Ｈを乗算してシンドローム$s1 = x_1 H^T$を演算する。そして、擬似シンドローム作成部１９１は、ビットパターンx_1を鍵不一致訂正部１９３へ出力し、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力する。

【００５０】

なお、これらの演算は、ｍｏｄ２の演算であり、H^Tは、検査行列Ｈの転置行列である。

【００５１】

不一致ビット検出部１９２は、擬似シンドローム作成部１９１からシンドロームｓ１を受け、無線装置３０の擬似シンドローム作成部１９１によって演算されたシンドローム$s2 = x_2 H^T$を受信処理部１４０から受ける。そして、不一致ビット検出部１９２は、シンドロームｓ１とシンドロームｓ２との差分ｓ＝ｓ１－ｓ２を演算する。

【００５２】

なお、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンの差分（鍵不一致のビットパターン）を$e = x_1 - x_2$とすると、$s = e H^T$の関係が成立する。ｓ＝０の場合、ｅ＝０となり、秘密鍵Ｋｓ１のビットパターンは、秘密鍵Ｋｓ２のビットパターンに一致する。

【００５３】

不一致ビット検出部１９２は、演算した差分ｓが０でないとき（即ち、ｅ≠０のとき）、鍵不一致のビットパターンｅを鍵不一致訂正部１９３へ出力する。

【００５４】

鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からビットパターンx_1を受け、不一致ビット検出部１９２から鍵不一致のビットパターンｅを受ける。そして、鍵不一致訂正部１９３は、ビットパターンx_1から鍵不一致のビットパターンｅを減算することにより相手方の秘密鍵のビットパターン$x_2 = x_1 - e$を演算する。

【００５５】

このように、鍵一致化部１９０は、秘密鍵Ｋｓ１，Ｋｓ２の不一致を誤りと見なして誤り訂正の応用により秘密鍵Ｋｓ１，Ｋｓ２の不一致を解消する。

【００５６】

この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるので、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

【００５７】

データ発生部１９４は、一致化後の鍵$x_2 = x_1 - e$を鍵不一致訂正部１９３から受けると、鍵x_2に基づいて鍵確認用データＤＣＦＭ３を発生させ、その発生させた鍵確認用データＤＣＦＭ３をデータ比較部１９５へ出力する。また、データ発生部１９４は、発生させた鍵確認用データＤＣＦＭ３を送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００５８】

なお、データ発生部１９４は、鍵一致確認部１７０のデータ発生部１７１による鍵確認用データＤＣＦＭ１の発生方法と同じ方法により鍵確認用データＤＣＦＭ３を発生する。

【００５９】

データ比較部１９５は、データ発生部１９４から鍵確認用データＤＣＦＭ３を受け、無線装置３０で発生された鍵確認用データＤＣＦＭ４を受信処理部１４０から受ける。そして、データ比較部１９５は、鍵確認用データＤＣＦＭ３を鍵確認用データＤＣＦＭ４と比較する。

【００６０】

データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に一致するとき、一致信号ＭＴＨを生成して結果処理部１９６へ出力する。

【００６１】

また、データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１９５は、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００６２】

結果処理部１９６は、データ比較部１９５から一致信号ＭＴＨを受けると、鍵不一致訂正部１９３から受けた鍵$x_2 = x_1 - e$を鍵記憶部１８０へ記憶する。

【００６３】

このように、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における確認方法と同じ方法によって一致化が施された鍵の一致を確認する。

【００６４】

図７は、受信信号プロファイルＲＳＳＩの概念図である。指向性設定部２３０の制御電圧発生回路２３１は、各々が電圧Ｖ１～Ｖ６からなる制御電圧ＣＬＶ１～ＣＬＶｎを順次発生してバラクタダイオード２３２へ出力する。この場合、電圧Ｖ１～Ｖ６は、それぞれ、アンテナ素子２１～２３，２５～２７に装荷される容量を変えるための電圧であり、０～２０Ｖの範囲で変えられる。

【００６５】

バラクタダイオード２３２は、パターンＰ１からなる制御電圧ＣＬＶ１に応じてアレーアンテナ２０の指向性をある１つの指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ１を検出する。

【００６６】

次に、バラクタダイオード２３２は、パターンＰ２からなる制御電圧ＣＬＶ２に応じてアレーアンテナ２０の指向性を別の指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ２を検出する。

【００６７】

以後、同様にして、バラクタダイオード２３２は、それぞれ、パターンＰ３～Ｐｎからなる制御電圧ＣＬＶ３～ＣＬＶｎに応じてアレーアンテナ２０の指向性を順次変える。そして、アレーアンテナ２０は、各々設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ３～ＷＩｎを順次検出する。

【００６８】

そして、プロファイル生成部１５０は、強度ＷＩ１～ＷＩｎからなる強度プロファイルを示す受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。

【００６９】

パターンＰ１～Ｐｎによってアレーアンテナ２０の指向性を複数個に順次切換えて無線装置３０から無線装置１０へデータを送信したとき、無線装置１０のプロファイル生成部１５０が受信信号プロファイルＲＳＳＩを生成する。

【００７０】

鍵作成部１６０は、プロファイル生成部１５０から受信信号プロファイルＲＳＳＩを受け、受信信号プロファイルＲＳＳＩから最大強度ＷＩｍａｘ（＝ＷＩ６）を検出する。そして、鍵作成部１６０は、最大強度ＷＩｍａｘ（＝ＷＩ６）によって受信信号プロファイルＲＳＳＩを規格化し、各強度ＷＩ１～ＷＩｎを多値化する。鍵作成部１６０は、多値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵Ｋｓ１またはＫｓ２を作成する。

【００７１】

図８は、図１に示す２つの無線装置１０，３０間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置３０の送信処理部１２０は、ｋ＝１を設定する（ステップＳ１）。そして、指向性設定部２３０は、パターンＰ１によりアレーアンテナ２０の指向性を１つの指向性に設定する（ステップＳ２）。

【００７２】

その後、無線装置１０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アンテナ１１を介して無線装置３０へ所定の信号を構成する電波を送信する（ステップＳ３）。

【００７３】

無線装置３０において、アレーアンテナ２０は、無線装置１０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アレーアンテナ２０から受けた電波の強度Ｉ１ｋを検出する（ステップＳ４）。

【００７４】

その後、無線装置３０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アレーアンテナ２０を介して無線装置１０へ所定の信号を構成する電波を送信する（ステップＳ５）。

【００７５】

無線装置１０において、アンテナ１１は、無線装置３０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ１１から受けた電波の強度Ｉ２ｋを検出する（ステップＳ６）。

【００７６】

その後、無線装置３０の送信処理部１２０は、ｋ＝ｋ＋１を設定し（ステップＳ７）、ｋ＝ｎであるか否かを判定する（ステップＳ８）。そして、ｋ＝ｎでないとき、ステップＳ２～Ｓ８が繰返し実行される。即ち、アレーアンテナ２０の指向性がパターンＰ１～Ｐｎによってｎ個に変えられて、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で所定の信号を構成する電波が送受信され、強度Ｉ１１～Ｉ１ｎ及びＩ２１～Ｉ２ｎが検出されるまで、ステップＳ２～Ｓ８が繰返し実行される。

【００７７】

ステップＳ８において、ｋ＝ｎであると判定されると、無線装置３０において、プロファイル生成部１５０は、強度Ｉ１１～Ｉ１ｎから受信信号プロファイルＲＳＳＩ１を作成して鍵作成部１６０へ出力する。

【００７８】

鍵作成部１６０は、受信信号プロファイルＲＳＳＩ１から最大強度ＷＩｍａｘ１を検出し、その検出した最大強度ＷＩｍａｘ１によって受信信号プロファイルＲＳＳＩ１を規格化し、強度Ｉ１１～Ｉ１ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ２を生成する（ステップＳ９）。

【００７９】

また、無線装置１０のプロファイル生成部１５０は、強度Ｉ２１～Ｉ２ｎから受信信号プロファイルＲＳＳＩ２を作成して鍵作成部１６０へ出力する。鍵作成部１６０は、受信

信号プロファイルＲＳＳＩ２から最大強度ＷＩｍａｘ２を検出し、その検出した最大強度ＷＩｍａｘ２によって受信信号プロファイルＲＳＳＩ２を規格化し、強度Ｉ２１～Ｉ２ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ１を生成する（ステップＳ１０）。

【００８０】

その後、無線装置１０において、鍵作成部１６０は、秘密鍵Ｋｓ１を鍵一致確認部１７０へ出力する。鍵一致確認部１７０のデータ発生部１７１は、上述した方法によって鍵確認用データＤＣＦＭ１を発生して送信処理部１２０及びデータ比較部１７２へ出力する。送信処理部１２０は、鍵確認用データＤＣＦＭ１に変調等の処理を施し、アンテナ部１３０を介して無線装置３０へ鍵確認用データＤＣＦＭ１を送信する。

【００８１】

そして、アンテナ部１３０は、無線装置３０において発生された鍵確認用データＤＣＦＭ２を無線装置３０から受信し、その受信した鍵確認用データＤＣＦＭ２を受信処理部１４０へ出力する。受信処理部１４０は、鍵確認用データＤＣＦＭ２に所定の処理を施し、鍵一致確認部１７０のデータ比較部１７２へ鍵確認用データＤＣＦＭ２を出力する。

【００８２】

データ比較部１７２は、データ発生部１７１からの鍵確認用データＤＣＦＭ１を受信処理部１４０からの鍵確認用データＤＣＦＭ２と比較する。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致しているとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。結果処理部１７３は、一致信号ＭＴＨに応じて、鍵作成部１６０からの秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。

【００８３】

一方、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、データ比較部１７２は、不一致信号ＮＭＴＨを生成して送信処理部１２０及び鍵一致化部１９０へ出力する。送信処理部１２０は、不一致信号ＮＭＴＨをアンテナ部１３０を介して無線装置３０へ送信する。そして、無線装置３０は、無線装置１０において秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたことを検知する。

【００８４】

これにより、無線装置１０における鍵一致の確認が終了する（ステップＳ１１）。

【００８５】

無線装置３０においても、無線装置１０と同じ動作によって鍵一致の確認が行なわれる（ステップＳ１２）。

【００８６】

ステップＳ１１において、秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたとき、無線装置１０において、鍵一致化部１９０の擬似シンドローム作成部１９１は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受ける。そして、擬似シンドローム作成部１９１は、不一致信号ＮＭＴＨに応じて、鍵作成部１６０から受けた秘密鍵Ｋｓ１のビットパターンx_1を検出し、その検出したビットパターンx_1のシンドローム$s1 = x_1 H^T$を演算する。

【００８７】

擬似シンドローム作成部１９１は、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力し、ビットパターンx_1を鍵不一致訂正部１９３へ出力する。

【００８８】

一方、無線装置３０は、ステップＳ１１において無線装置１０から不一致信号ＮＭＴＨを受信し、その受信した不一致信号ＮＭＴＨに応じて、シンドローム$s2 = x_2 H^T$を演算して無線装置１０へ送信する。

【００８９】

無線装置１０のアンテナ部１３０は、無線装置３０からシンドローム$s2 = x_2 H^T$を受信して受信処理部１４０へ出力する。受信処理部１４０は、シンドローム$s2 = x_2 H^T$に対して所定の処理を施し、シンドローム$s2 = x_2 H^T$を鍵一致化部１９０へ出力する。

【００９０】
鍵一致化部１９０の不一致ビット検出部１９２は、受信処理部１４０から無線装置３０において作成されたシンドロームｓ２＝$x_2 H^T$を受ける。そして、不一致ビット検出部１９２は、無線装置１０で作成されたシンドロームｓ１＝$x_1 H^T$と無線装置３０において作成されたシンドロームｓ２＝$x_2 H^T$との差分ｓ＝ｓ１－ｓ２を演算する。
【００９１】
その後、不一致ビット検出部１９２は、ｓ≠０であることを確認し、鍵不一致のビットパターンｅ＝$x_1 - x_2$をｓ＝ｅH^Tに基づいて演算し、その演算した鍵不一致のビットパターンｅを鍵不一致訂正部１９３へ出力する。
【００９２】
鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からのビットパターンx_1と、不一致ビット検出部１９２からの鍵不一致のビットパターンｅとに基づいて、無線装置３０において作成された秘密鍵Ｋｓ２のビットパターン$x_2 = x_1 - e$を演算する。
【００９３】
そして、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における鍵一致確認の動作と同じ動作によって、一致化された鍵$x_2 = x_1 - e$の一致を確認する。
【００９４】
これにより、鍵不一致対策が終了する（ステップＳ１３）。
【００９５】
無線装置３０においても、無線装置１０と同じ動作によって鍵不一致対策が行なわれる（ステップＳ１４）。
【００９６】
ステップＳ１１において、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することが確認されたとき、またはステップＳ１３において鍵不一致対策がなされたとき、暗号部２００は、鍵記憶部１８０から秘密鍵Ｋｓ１を読出して送信データを暗号化し、暗号化した送信データを送信処理部１２０へ出力する。そして、送信処理部１２０は、暗号化された送信データに変調等を施し、アンテナ部１３０を介して暗号化された送信データを無線装置３０へ送信する。
【００９７】
また、アンテナ部１３０は、暗号化された送信データを無線装置３０から受信し、その受信した暗号化された送信データを受信処理部１４０へ出力する。受信処理部１４０は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部２１０へ出力する。
【００９８】
復号部２１０は、受信処理部１４０からの暗号化された送信データを復号して受信データを取得する。
【００９９】
これにより、秘密鍵Ｋｓ１による暗号・復号が終了する（ステップＳ１５）。
【０１００】
無線装置３０においても、無線装置１０と同じ動作によって秘密鍵Ｋｓ２による暗号・復号が行なわれる（ステップＳ１６）。そして、一連の動作が終了する。
【０１０１】
上述したステップＳ３，Ｓ４に示す動作は、無線装置３０において受信信号プロファイルＲＳＳＩ１を生成するための電波を無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ送信し、かつ、無線装置３０において電波の強度Ｉ１ｋを検出する動作であり、ステップＳ５，Ｓ６に示す動作は、無線装置１０において受信信号プロファイルＲＳＳＩ２を生成するための電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、かつ、無線装置１０において電波の強度Ｉ２ｋを検出する動作である。そして、所定の信号を構成する電波の無線装置１０のアンテナ１１から無線装

置３０のアレーアンテナ２０への送信及び所定の信号を構成する電波の無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１への送信は、アレーアンテナ２０の指向性を１つの指向性に設定して交互に行なわれる。つまり、所定の信号を構成する電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で時分割復信（ＴＤＤ）により送受信される。

【０１０２】

従って、アレーアンテナ２０の指向性を１つの指向性に設定して無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ所定の信号を構成する電波を送信し、無線装置３０において電波の強度Ｉ１ｋを検出した直後に、同じ所定の信号を構成する電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、無線装置１０において電波の強度Ｉ２ｋを検出することができる。その結果、無線装置１０，３０間において同じ伝送路特性を確保して所定の信号を構成する電波を無線装置１０，３０間で送受信でき、電波の可逆性により電波の強度Ｉ１１～Ｉ１ｎをそれぞれ電波の強度Ｉ２１～Ｉ２ｎに一致させることができる。そして、無線装置１０において作成される秘密鍵Ｋｓ１を無線装置３０において作成される秘密鍵Ｋｓ２に容易に一致させることができる。

【０１０３】

また、所定の信号を構成する電波は、無線装置１０，３０間で時分割復信（ＴＤＤ）により送受信されるので、電波の干渉を抑制して１つのアレーアンテナ２０を介して所定の信号を構成する電波を無線装置１０，３０間で送受信できる。

【０１０４】

更に、アレーアンテナ２０の指向性を１つの指向性に設定して無線装置１０，３０間で所定の信号を構成する電波を送受信し、秘密鍵Ｋｓ１，Ｋｓ２を作成するための受信信号プロファイルＲＳＳＩ１，ＲＳＳＩ２を生成するので、図１に示すようにアレーアンテナ２０を装着した無線装置３０の近傍に盗聴装置５０が配置されていても、盗聴装置５０による秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０１０５】

即ち、盗聴装置５０は、アンテナ１１及びアレーアンテナ２０から送信された電波をアンテナ５１を介して受信するが、アレーアンテナ２０は指向性を各指向性に設定して電波を送受信するので、アンテナ１１とアレーアンテナ２０との間で送受信される電波は、アンテナ１１またはアレーアンテナ２０とアンテナ５１との間で送受信される電波と異なり、盗聴装置５０は、無線装置３０が送受信する電波と同じ電波を送受信できず、電波の強度Ｉ１ｋと同じ強度を得ることができない。その結果、盗聴装置５０は、秘密鍵Ｋｓ１，Ｋｓ２を盗聴することができない。

【０１０６】

従って、この発明においては、電気的に指向性を切換え可能なアレーアンテナ２０を盗聴装置５０の近傍に配置された無線装置３０に装着することを特徴とする。

【０１０７】

更に、鍵確認用データＤＣＦＭ１～４は、秘密鍵Ｋｓ１，Ｋｓ２に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データＤＣＦＭ１～４が盗聴されても秘密鍵Ｋｓ１，Ｋｓ２が解読される危険性を極めて低くできる。

【０１０８】

更に、シンドロームｓ１，ｓ２は、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンを示す鍵x_1，x_2に検査行列Ｈの転置行列H^Tを乗算して得られるので、シンドロームｓ１，ｓ２が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

【０１０９】

なお、無線装置１０，３０間で通信を行なう動作は、実際には、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）によって行なわれ、無線装置１０に搭載されたＣＰＵは、図８に示す各ステップＳ３，Ｓ６，Ｓ１０，Ｓ１１，Ｓ１３，Ｓ１５を備えるプ

ログラムをＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）から読出し、無線装置３０に搭載されたＣＰＵは、図８に示す各ステップＳ１，Ｓ２，Ｓ４，Ｓ５，Ｓ７，Ｓ８，Ｓ９，Ｓ１２，Ｓ１４，Ｓ１６を備えるプログラムをＲＯＭから読出し、無線装置１０，３０に搭載された２つのＣＰＵは、その読出したプログラムを実行して図８に示すフローチャートに従って無線装置１０，３０間で通信を行なう。

【０１１０】

従って、ＲＯＭは、無線装置１０，３０間で通信を行なう動作をコンピュータ（ＣＰＵ）に実行させるためのプログラムを記録したコンピュータ（ＣＰＵ）読取り可能な記録媒体に相当する。

【０１１１】

そして、図８に示す各ステップを備えるプログラムは、アレーアンテナ２０の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置１０，３０間における通信をコンピュータ（ＣＰＵ）に実行させるプログラムである。

【０１１２】

上記においては、電気的に指向性を切換え可能なアレーアンテナ２０を無線装置３０のみに装着すると説明したが、この発明においては、アレーアンテナ２０は、無線装置１０及び３０の両方に装着されてもよい。

【０１１３】

即ち、この発明においては、アレーアンテナ２０は、２つの無線装置１０，３０のうち、少なくとも一方の無線装置に装着されていればよい。そして、アレーアンテナ２０を装着した無線装置は、好ましくは、盗聴装置５０の近傍に配置される。

【０１１４】

また、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、無線装置１０，３０間の通信環境に応じて決定されてもよい。即ち、無線装置１０，３０間の通信環境が盗聴し易い環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、無線装置１０，３０間の通信環境が盗聴しにくい環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

【０１１５】

更に、定期的に秘密鍵Ｋｓ１，Ｋｓ２の鍵長を変えるようにしてもよい。

【０１１６】

更に、無線装置１０，３０間で送受信する情報の機密性に応じて秘密鍵Ｋｓ１、Ｋｓ２の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

【０１１７】

そして、この鍵長は、アレーアンテナ２０の指向性を変化させる個数、即ち、制御電圧ＣＬＶ１～ＣＬＶｎの個数により制御される。秘密鍵Ｋｓ１，Ｋｓ２は、検出された電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数からなるビットパターンを有し、電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数は、アレーアンテナ２０の指向性を変化させる個数に等しいからである。つまり、制御電圧ＣＬＶ１～ＣＬＶｎの個数により秘密鍵Ｋｓ１，Ｋｓ２の鍵長を制御できる。

【０１１８】

このように、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、電気的に指向性を切換え可能なアレーアンテナ２０の指向性を変化させる個数によって決定される。

【０１１９】

更に、上記においては、２つの無線装置間において秘密鍵を生成する場合、即ち、１つの無線装置が１つの無線装置と通信する場合について説明したが、この発明は、これに限らず、１つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、１つの無線装置は、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成する。１つの無線装置は、アレーアンテナ２０の指向性の切換パターンを

１つに固定して複数の無線装置との間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって１つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

【０１２０】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【産業上の利用可能性】

【０１２１】

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。

【図面の簡単な説明】

【０１２２】

【図１】この発明の実施の形態による無線通信システムの概略図である。

【図２】図１に示す一方の無線装置の概略ブロック図である。

【図３】図１に示す他方の無線装置の概略ブロック図である。

【図４】図３に示す指向性設定部の概略ブロック図である。

【図５】図２及び図３に示す鍵一致確認部の概略ブロック図である。

【図６】図２及び図３に示す鍵一致化部の概略ブロック図である。

【図７】受信信号プロファイルＲＳＳＩの概念図である。

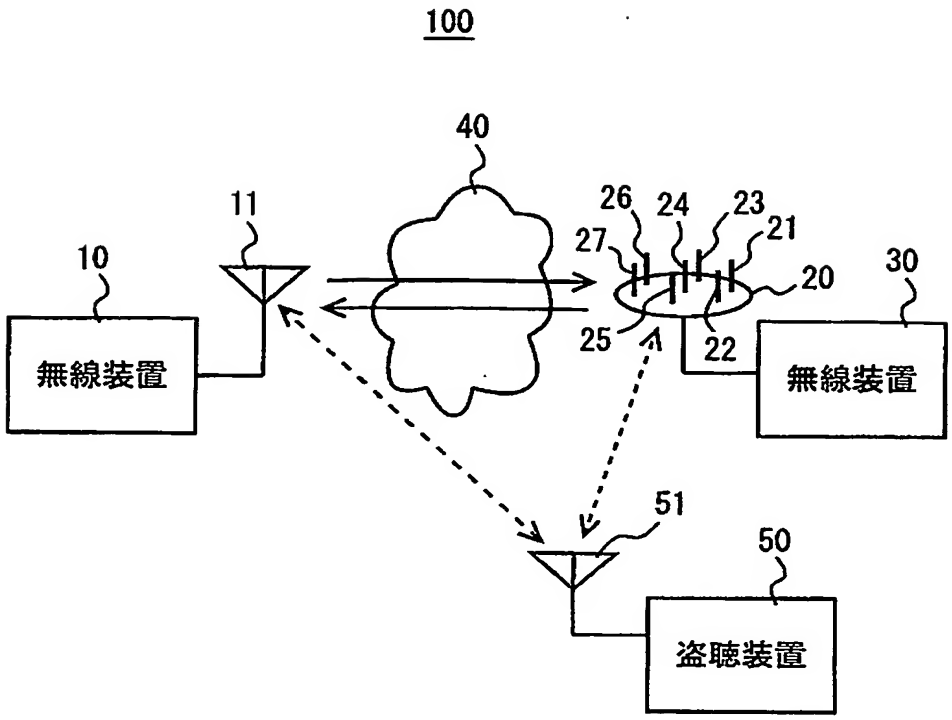
【図８】図１に示す２つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

【符号の説明】

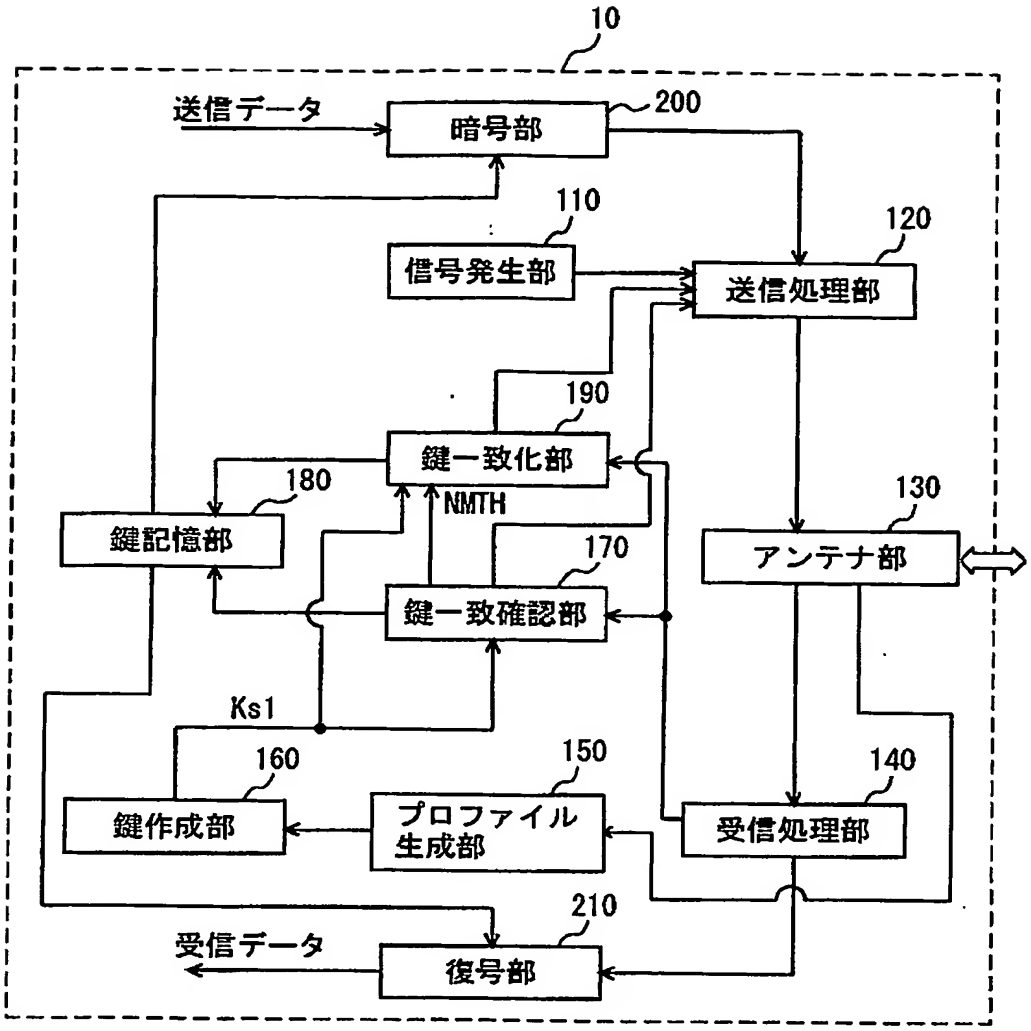
【０１２３】

１０，３０　無線装置、１１，５１　アンテナ、２０　アレーアンテナ、２１～２７　アンテナ素子、４０　中間物、５０　盗聴装置、１００　無線通信システム、１１０　信号発生部、１２０　送信処理部、１３０，２２０　アンテナ部、１４０　受信処理部、１５０　プロファイル生成部、１６０　鍵作成部、１７０　鍵一致確認部、１７１，１９４　データ発生部、１７２，１９５　データ比較部、１７３，１９６　結果処理部、１８０　鍵記憶部、１９０　鍵一致化部、１９１　擬似シンドローム作成部、１９２　不一致ビット検出部、１９３　鍵不一致訂正部、２００　暗号部、２１０　復号部、２３０　指向性設定部、２３１　制御電圧発生回路、２３２　バラクタダイオード。

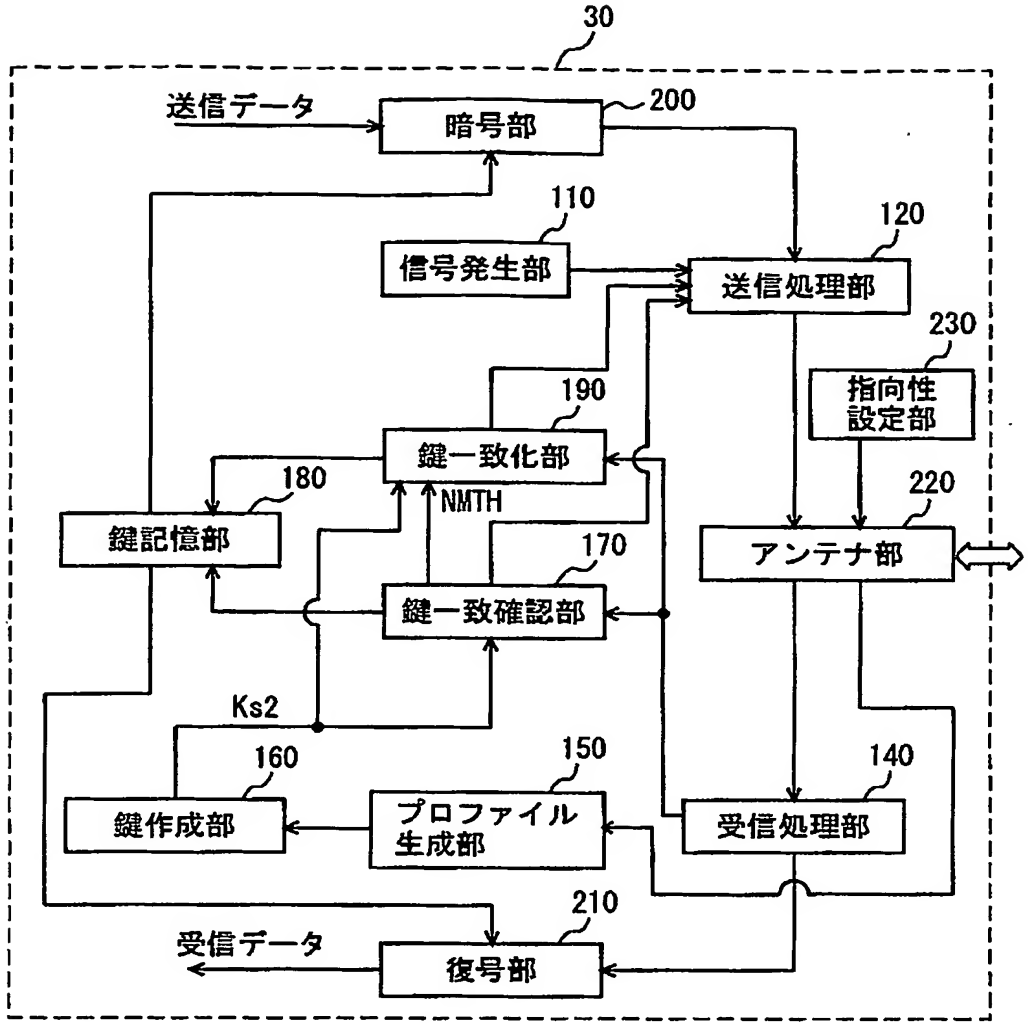
【書類名】図面
【図１】



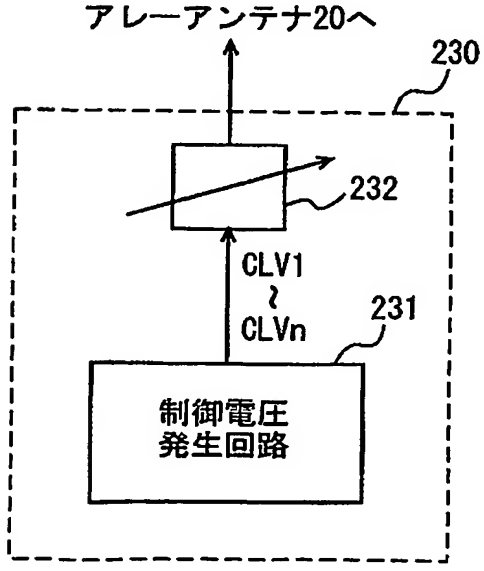
【図２】


10
送信データ
暗号部
200
110
信号発生部
120
送信処理部
190
鍵一致化部
180
NMTH
鍵記憶部
130
アンテナ部
170
鍵一致確認部
Ks1
160
150
140
鍵作成部
プロファイル
生成部
受信処理部
210
受信データ
復号部

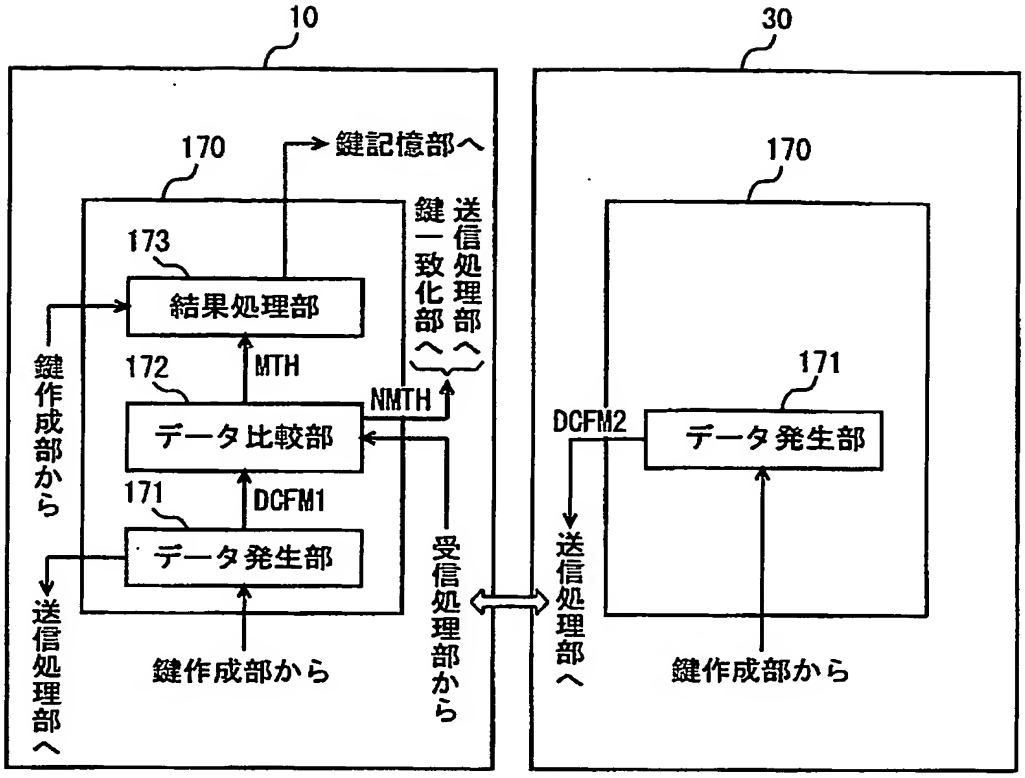
【図３】


30
送信データ
暗号部
200
110
信号発生部
120
送信処理部
230
指向性
設定部
190
鍵一致化部
180
NMTH
220
鍵記憶部
アンテナ部
170
鍵一致確認部
Ks2
160
150
140
鍵作成部
プロファイル
生成部
受信処理部
210
受信データ
復号部

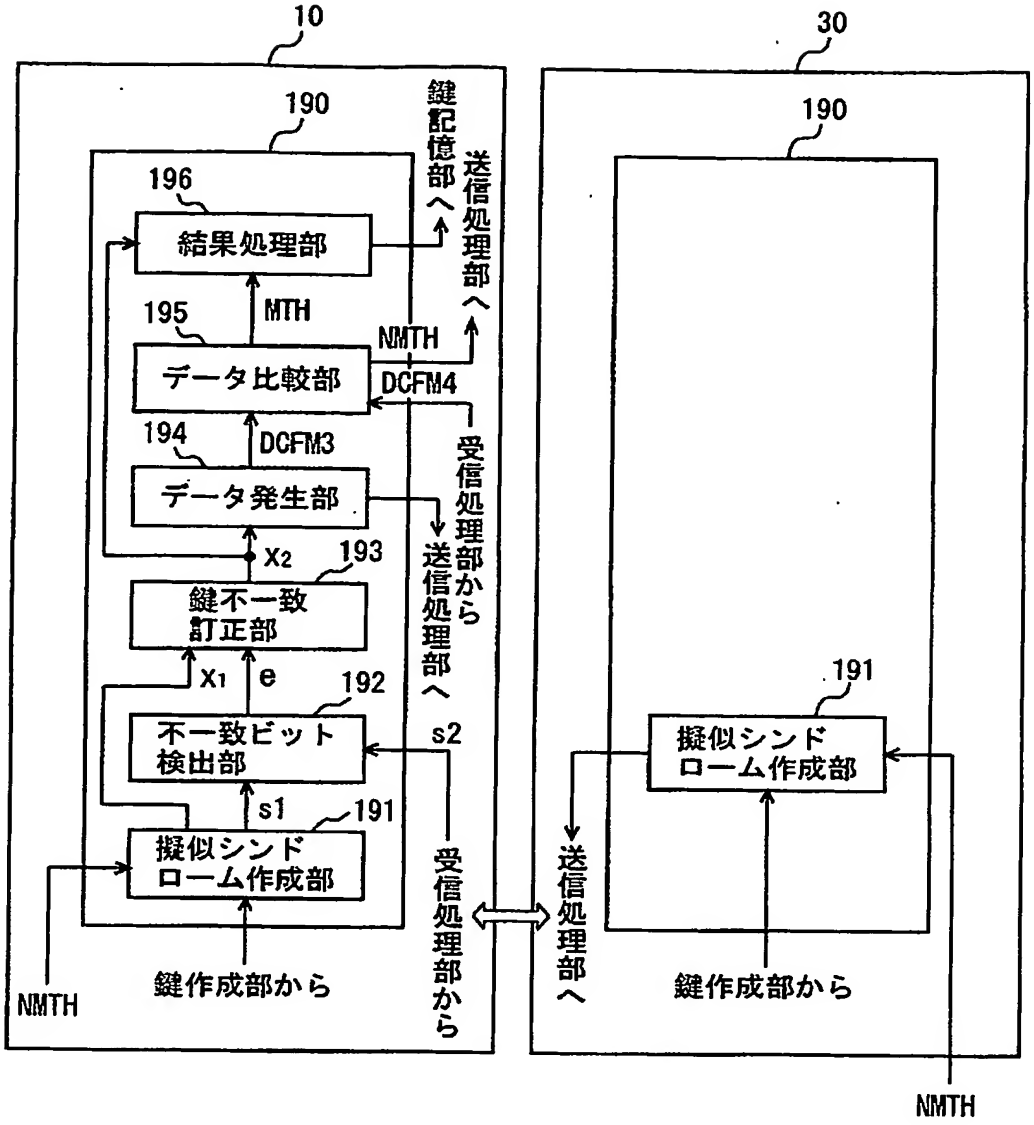
【図４】


アレーアンテナ20へ
230
232
CLV1
～
CLVn
231
制御電圧
発生回路

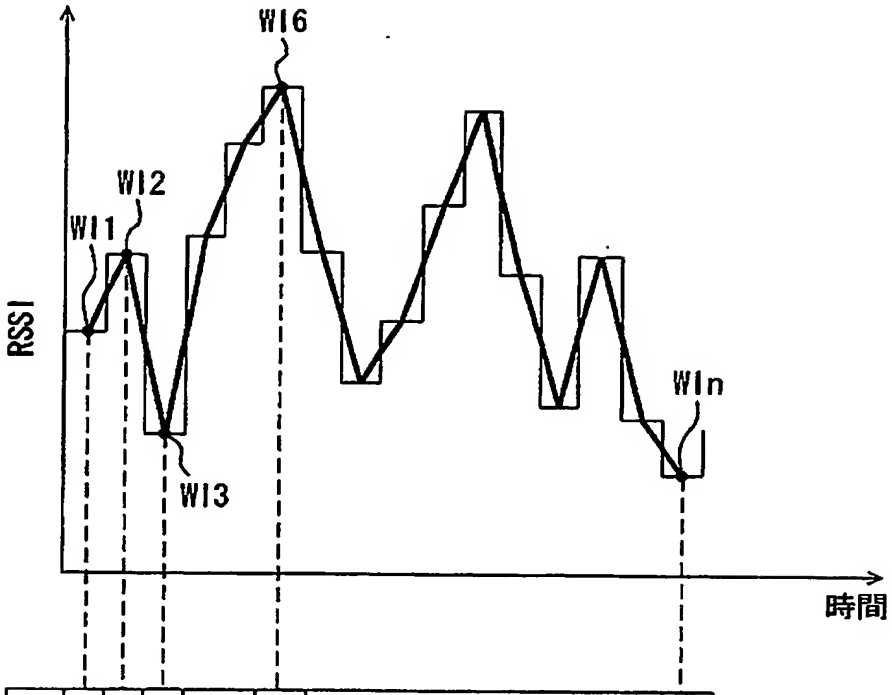
【図５】


10
30
170
鍵記憶部へ
送信処理部へ
鍵一致化部へ
173
結果処理部
鍵作成部から
172
MTH
NMTH
データ比較部
171
DCFM1
データ発生部
送信処理部へ
鍵作成部から
受信処理部から
170
171
DCFM2
データ発生部
送信処理部へ
鍵作成部から

【図６】

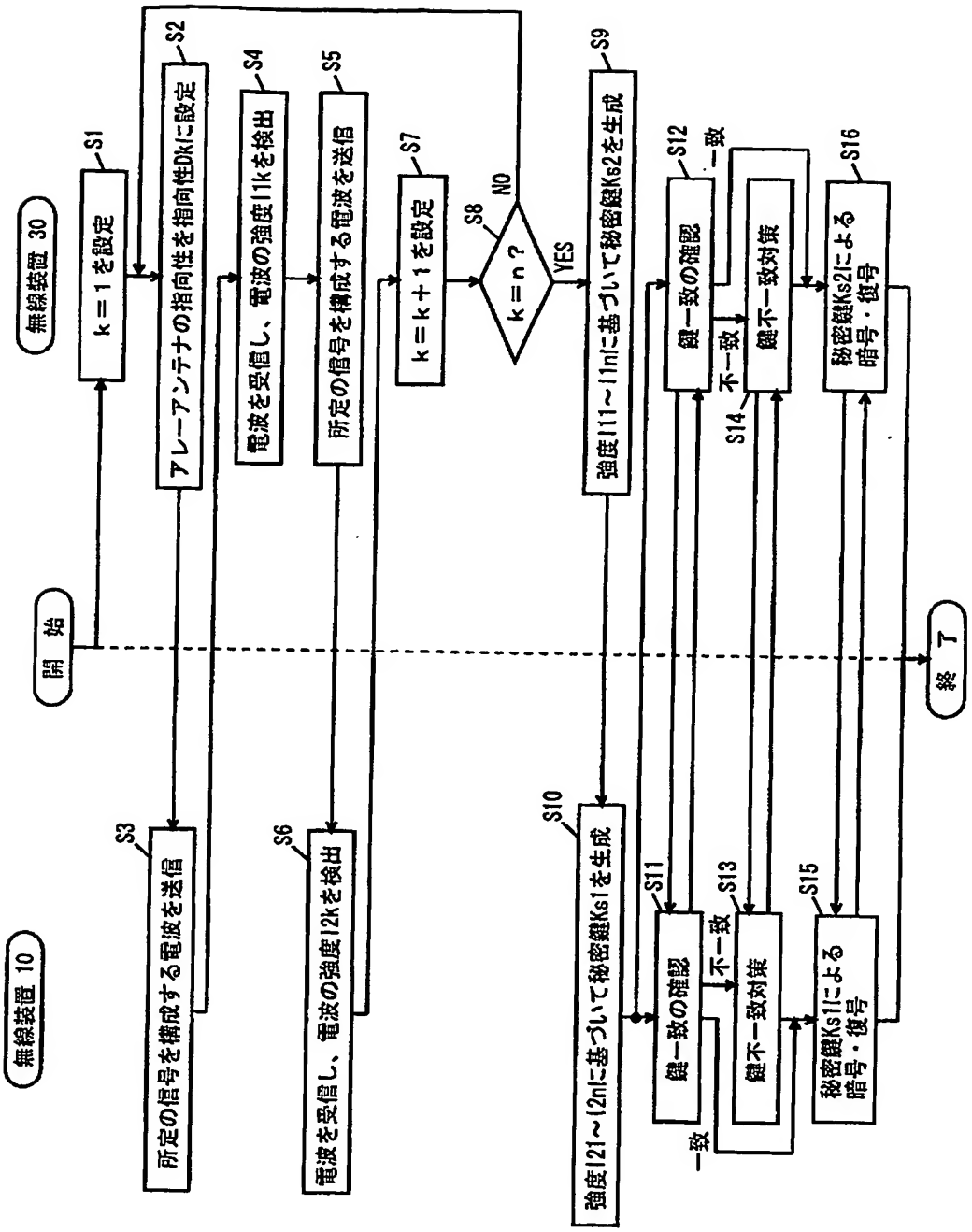

10
30
190
190
196
結果処理部
195
MTH
データ比較部
194
DCFM3
データ発生部
193
鍵不一致
訂正部
192
不一致ビット
検出部
191
擬似シンド
ローム作成部
191
擬似シンド
ローム作成部
鍵記憶部へ
送信処理部へ
NMTH
DCFM4
受信処理部から
送信処理部へ
X2
X1
e
s2
s1
受信処理部から
送信処理部へ
NMTH
鍵作成部から
鍵作成部から
NMTH

【図７】



	P1	P2	P3	..	P6	.....	Pn
V1	0	1	2		0		0
V2	0	0	0		1		1
V3	1	0	0		0		0
V4	0	0	0	..	0	.....	2
V5	0	0	0		0		0
V6	0	0	0		0		1

【図８】


無線装置 30
無線装置 10
開 始
終 了
k＝１を設定
アレーアンテナの指向性を指向性Dkに設定
所定の信号を構成する電波を送信
電波を受信し、電波の強度I1kを検出
所定の信号を構成する電波を送信
電波を受信し、電波の強度I2kを検出
k＝k＋１を設定
k＝n？
NO
YES
強度I11～I1nに基づいて秘密鍵Ks2を生成
強度I21～I2nに基づいて秘密鍵Ks1を生成
鍵一致の確認
鍵一致の確認
不一致
不一致
一致
一致
鍵不一致対策
鍵不一致対策
秘密鍵Ks2による暗号・復号
秘密鍵Ks1による暗号・復号
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16

【書類名】要約書
【要約】
【課題】　秘密鍵の盗聴を抑制可能な無線通信システムを提供する。
【解決手段】　無線通信システム１００は、無線装置１０，３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０及び３０は、アレーアンテナ２０の指向性を複数個に変えながら時分割復信（ＴＤＤ）により所定の信号をアンテナ１１及びアレーアンテナ２０を介して相互に送受信する。そして、無線装置１０及び３０は、受信した複数の電波の強度を検出して複数の強度のプロファイルを示す受信信号プロファイルＲＳＳＩ１，２をそれぞれ作成する。無線装置１０及び３０は、それぞれ、受信信号プロファイルＲＳＳＩ１，２の複数の強度を多値化し、その多値化した複数の値をビットパターンとする秘密鍵Ｋｓ１，Ｋｓ２を作成する。
【選択図】　図１

特願２００３－３１２１５６

出　願　人　履　歴　情　報

識別番号　　［５０３０２７９３１］

１．変更年月日　　２００３年　４月　４日
［変更理由］　　住所変更
住　所　　京都府京都市上京区今出川通烏丸東入玄武町６０１
氏　名　　学校法人同志社

特願２００３－３１２１５６

出願人履歴情報

識別番号　［３９３０３１５８６］

１．変更年月日　２０００年　３月２７日
［変更理由］　住所変更
住　所　京都府相楽郡精華町光台二丁目２番地２
氏　名　株式会社国際電気通信基礎技術研究所

PCT/JP2004/002228

日本国特許庁
JAPAN PATENT OFFICE

25.2.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月　５日

出願番号
Application Number: 特願２００４－０００５３３

[ST. 10/C]: [ＪＰ２００４－０００５３３]

出願人
Applicant(s): 学校法人同志社
株式会社国際電気通信基礎技術研究所

２００４年　３月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０２５１１７

【書類名】　特許願
【整理番号】　1032333
【提出日】　平成16年 1月 5日
【あて先】　特許庁長官殿
【国際特許分類】　H04B 13/00
【発明者】
　【住所又は居所】　京都府京田辺市多々羅都谷１－３　同志社大学内
　【氏名】　笹岡　秀一
【発明者】
　【住所又は居所】　京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内
　【氏名】　青野　智之
【発明者】
　【住所又は居所】　京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内
　【氏名】　大平　孝
【特許出願人】
　【識別番号】　503027931
　【住所又は居所】　京都府京都市上京区今出川通烏丸東入玄武町６０１番地
　【氏名又は名称】　学校法人同志社
【特許出願人】
　【識別番号】　393031586
　【住所又は居所】　京都府相楽郡精華町光台二丁目２番地２
　【氏名又は名称】　株式会社国際電気通信基礎技術研究所
【代理人】
　【識別番号】　100064746
　【弁理士】
　【氏名又は名称】　深見　久郎
【選任した代理人】
　【識別番号】　100085132
　【弁理士】
　【氏名又は名称】　森田　俊雄
【選任した代理人】
　【識別番号】　100083703
　【弁理士】
　【氏名又は名称】　仲村　義平
【選任した代理人】
　【識別番号】　100096781
　【弁理士】
　【氏名又は名称】　堀井　豊
【選任した代理人】
　【識別番号】　100098316
　【弁理士】
　【氏名又は名称】　野田　久登
【選任した代理人】
　【識別番号】　100109162
　【弁理士】
　【氏名又は名称】　酒井　將行
【国等の委託研究の成果に係る記載事項】　平成１５年度通信・放送機構、研究テーマ「自律分散型無線ネットワークの研究開発」に関する委託研究、産

業活力再生特別措置法第３０条の適用を受ける特許出願

【手数料の表示】
　【予納台帳番号】　008693
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0315129
　【包括委任状番号】　0005582

【書類名】特許請求の範囲
【請求項１】
指向性を電気的に切換え可能な第１のアンテナと、
第２のアンテナと、
前記第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する第１及び第２の無線装置とを備え、
前記第１の無線装置は、前記第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第２の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成し、
前記第２の無線装置は、前記第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第１の無線装置が前記所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて前記第１の秘密鍵と同じ第２の秘密鍵を生成する、無線通信システム。
【請求項２】
前記第１の無線装置は、前記第１のアンテナが無指向性に制御されたときに前記第２の無線装置との間で前記無線伝送路を確立し、前記無線伝送路が確立した後、前記第１のアンテナの指向性を前記複数個に変えながら前記第２の無線装置との間で前記複数のデータを送受信する、請求項１に記載の無線通信システム。
【請求項３】
前記第１の無線装置は、前記第２の無線装置との間における前記各データの送受信において、前記第１のアンテナの指向性を更新して前記第２の無線装置から前記データを受信し、前記更新した前記第１のアンテナの指向性を維持して前記受信したデータを前記第２の無線装置へ送信する、請求項２に記載の無線通信システム。
【請求項４】
前記所定の通信プロトコルは、複数の階層からなり、
前記複数のデータは、前記複数の階層のうち、前記データを前記電気信号に変換する階層におけるデータフォーマットに含まれ、
前記データを前記電気信号に変換する階層は、複数の通信プロトコルに共通な階層である、請求項２または請求項３に記載の無線通信システム。
【請求項５】
前記複数のデータの各々は、前記第１および第２の無線装置により受信された電波の強度を検出する区間と、前記第１のアンテナの指向性を変更する区間とからなる、請求項１から請求項４のいずれか１項に記載の無線通信システム。
【請求項６】
前記第１の無線装置は、前記生成した第１の秘密鍵が前記第２の秘密鍵に不一致であるとき、前記第１の秘密鍵を前記第２の秘密鍵に一致させる、請求項１から請求項５のいずれか１項に記載の無線通信システム。
【請求項７】
前記第１のアンテナは、盗聴者の端末に近接して配置された第１の無線装置に設置される、請求項１から請求項６のいずれか１項に記載の無線通信システム。
【請求項８】
前記第１及び第２の無線装置は、前記第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する、請求項１から請求項７のいずれか１項に記載の無線通信システム。

【書類名】明細書
【発明の名称】無線通信システム
【技術分野】
【０００１】
この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システムに関するものである。
【背景技術】
【０００２】
最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来から情報を暗号化して送信することが行なわれている。
【０００３】
情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性は高いが、大容量のデータの暗号化には向かない。
【０００４】
一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。
【０００５】
そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、２つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（非特許文献１）。
【０００６】
この方法は、２つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて生成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。
【０００７】
このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを２つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。
【非特許文献１】堀池　元樹、笹岡　秀一，「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」，信学技報，社団法人　電子情報通信学会，２００２年１０月，TECHNICAL REPORT OF IEICE RCS2002-173，ｐ．７－１２
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかし、２つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。
【０００９】
そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、秘密鍵の盗聴を抑制することができる無線通信システムを提供することである。
【課題を解決するための手段】
【００１０】
この発明によれば、無線通信システムは、第１および第２のアンテナと、第１および第２の無線装置とを備える。第１のアンテナは、指向性を電気的に切換え可能なアンテナで

ある。第１および第２の無線装置は、第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第１の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第２の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成する。また、第２の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第１の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて第１の秘密鍵と同じ第２の秘密鍵を生成する。

【００１１】

好ましくは、第１の無線装置は、第１のアンテナが無指向性に制御されたときに第２の無線装置との間で無線伝送路を確立し、無線伝送路が確立した後、第１のアンテナの指向性を複数個に変えながら第２の無線装置との間で複数のデータを送受信する。

【００１２】

好ましくは、第１の無線装置は、第２の無線装置との間における各データの送受信において、第１のアンテナの指向性を更新して第２の無線装置からデータを受信し、更新した第１のアンテナの指向性を維持して受信したデータを第２の無線装置へ送信する。

【００１３】

好ましくは、所定の通信プロトコルは、複数の階層からなる。複数のデータは、複数の階層のうち、データを電気信号に変換する階層におけるデータフォーマットに含まれる。そして、データを電気信号に変換する階層は、複数の通信プロトコルに共通な階層である。

【００１４】

好ましくは、複数のデータの各々は、第１および第２の無線装置により受信された電波の強度を検出する区間と、第１のアンテナの指向性を変更する区間とからなる。

【００１５】

好ましくは、第１の無線装置は、生成した第１の秘密鍵が第２の秘密鍵に不一致であるとき、第１の秘密鍵を第２の秘密鍵に一致させる。

【００１６】

好ましくは、第１のアンテナは、盗聴者の端末に近接して配置された第１の無線装置に設置される。

【００１７】

好ましくは、第１及び第２の無線装置は、第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

【発明の効果】

【００１８】

この発明による無線通信システムにおいては、指向性を電気的に切換え可能なアンテナを介して２つの無線装置間で所定のデータが所定の通信プロトコルに従って送受信される。そして、このアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが２つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて２つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、２つの無線装置間に形成される伝送路に固有である。即ち、２つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、２つの端末装置で生成される受信信号プロファイルと異なる。

【００１９】

従って、この発明によれば、２つの無線装置において作成される秘密鍵の盗聴を抑制できる。また、２つの無線装置において作成される秘密鍵を生成するためのデータを所定の

通信プロトコルに従って送受信できる。

【発明を実施するための最良の形態】

【００２０】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２１】

図１は、この発明の実施の形態による無線通信システムの概略図である。無線通信システム１００は、無線装置１０，３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０は、例えば、ユーザの移動体通信端末である。また、無線装置３０は、例えば、無線アクセスポイントである。そして、無線装置１０は、無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）のプロトコルであるＩＥＥＥ８０２．１１ｂまたはＩＥＥＥ８０２．１１ｇに従って無線装置３０との間で通信を行なう。

【００２２】

アンテナ１１は、無線装置１０に装着される。そして、アンテナ１１は、全方位性のアンテナである。アレーアンテナ２０は、アンテナ素子２１～２７を備える。アンテナ素子２４は、給電素子であり、残るアンテナ素子２１～２３，２５～２７は、無給電素子である。そして、アンテナ素子２４は、アンテナ素子２１～２３，２５～２７によって取り囲まれている。無給電素子であるアンテナ素子２１～２３，２５～２７のそれぞれには、可変容量素子であるバラクタダイオード（図示せず）が装荷されており、そのバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ２０は、適応ビーム形成が可能である。

【００２３】

即ち、アレーアンテナ２０は、無線装置３０に含まれるバラクタダイオードに印加する直流電圧を変えることによって指向性が変えられる。従って、アレーアンテナ２０は、電気的に指向性を切換え可能なアンテナである。そして、アレーアンテナ２０は、無線装置３０に装着される。

【００２４】

無線装置１０と無線装置３０との間で通信が行われる場合、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による影響を受けて伝搬する。中間物４０としては、反射物及び障害物が想定される。中間物４０が反射物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって反射されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。また、中間物４０が障害物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって回折されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。

【００２５】

このように、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による反射を受けて反射波として伝搬したり、中間物４０による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬した電波がどのような成分により構成されるかによって無線装置１０と無線装置３０との間の伝送路の特性が決定される。

【００２６】

この発明においては、無線装置１０と無線装置３０との間で通信が行なわれる場合、アレーアンテナ２０の指向性を複数個に変えて時分割復信（ＴＤＤ：Ｔｉｍｅ　Ｄｉｖｉｓｉｏｎ　Ｄｕｐｌｅｘ）等により所定のデータが同一の周波数で無線装置１０，３０間で

送受信される。そして、無線装置１０，３０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルＲＳＳＩを生成し、その生成した受信信号プロファイルＲＳＳＩに基づいて秘密鍵を作成する。

【００２７】

秘密鍵が無線装置１０，３０において生成されると、無線装置１０，３０は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

【００２８】

図２は、図１に示す一方の無線装置１０の内部構成を示す概略ブロック図である。無線装置１０は、信号発生部１１０と、送信処理部１２０と、アンテナ部１３０と、受信処理部１４０と、プロファイル生成部１５０と、鍵作成部１６０と、鍵一致確認部１７０と、鍵記憶部１８０と、鍵一致化部１９０と、暗号部２００と、復号部２１０とを含む。

【００２９】

信号発生部１１０は、秘密鍵を生成するときに無線装置３０へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部１２０へ出力する。送信処理部１２０は、暗号部２００から暗号化データを受けると、その受けた暗号化データに対して変調、周波数変換および増幅等を施してアンテナ部１３０から送信する。また、送信処理部１２０は、信号発生部１１０から所定の信号を受けると、所定の信号を所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層を構成するデータフォーマットに含め、変調、周波数変換および増幅等を施してアンテナ部１３０から送信する。

【００３０】

アンテナ部１３０は、図１に示すアンテナ１１からなり、送信処理部１２０からの信号を無線装置３０へ送信し、無線装置３０からの信号を受信して受信処理部１４０またはプロファイル生成部１５０へ供給する。

【００３１】

受信処理部１４０は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部１４０は、受信処理を行なった信号を必要に応じて鍵一致確認部１７０、鍵一致化部１９０及び復号部２１０へ出力する。

【００３２】

プロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部１３０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。

【００３３】

鍵作成部１６０は、プロファイル生成部１５０からの受信信号プロファイルＲＳＳＩに基づいて秘密鍵Ｋｓ１を作成する。そして、鍵作成部１６０は、作成した秘密鍵Ｋｓ１を鍵一致確認部１７０及び鍵一致化部１９０へ出力する。

【００３４】

鍵一致確認部１７０は、所定の信号を送信処理部１２０、アンテナ部１３０及び受信処理部１４０を介して無線装置３０と送受信し、鍵作成部１６０によって作成された秘密鍵Ｋｓ１が無線装置３０において作成された秘密鍵Ｋｓ２に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致すると確認したとき、秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。また、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に不一致であることを確認したとき、不一致信号ＮＭＴＨを生成して鍵一致化部１９０へ出力する。

【００３５】

鍵記憶部１８０は、鍵一致確認部１７０及び鍵一致化部１９０からの秘密鍵Ｋｓ１を記憶する。また、鍵記憶部１８０は、記憶した秘密鍵Ｋｓ１を暗号部２００及び復号部２１０へ出力する。なお、鍵記憶部１８０は、秘密鍵Ｋｓ１を一時的、例えば、無線装置３０

との通信の間だけ記憶するようにしてもよい。

【００３６】

鍵一致化部１９０は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受けると、後述する方法によって秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる。そして、鍵一致化部１９０は、一致させた秘密鍵が秘密鍵Ｋｓ２に一致することを鍵一致確認部１７０における方法と同じ方法によって確認する。

【００３７】

暗号部２００は、送信データを鍵記憶部１８０に記憶された秘密鍵Ｋｓ１によって暗号して送信処理部１２０へ出力する。復号部２１０は、受信処理部１４０からの信号を鍵記憶部１８０からの秘密鍵Ｋｓ１によって復号して受信データを生成する。

【００３８】

図３は、図１に示す他方の無線装置３０の内部構成を示す概略ブロック図である。無線装置３０は、無線装置１０のアンテナ部１３０をアンテナ部２２０に代え、指向性設定部２３０を追加したものであり、その他は、無線装置１０と同じである。

【００３９】

アンテナ部２２０は、図１に示すアレーアンテナ２０からなる。アンテナ部２２０は、送信処理部１２０からの信号を指向性設定部２３０によって設定された無指向性または指向性で無線装置１０へ送信する。すなわち、アンテナ部２２０は、オムニアンテナまたは指向性アンテナとして機能し、送信処理部１２０からの信号を無線装置１０へ送信する。また、アンテナ部２２０は、無線装置１０からの信号を指向性設定部２３０によって設定された指向性で受信して受信処理部１４０またはプロファイル生成部１５０へ出力する。

【００４０】

指向性設定部２３０は、アンテナ部２２０の指向性を設定する機能を持ち、無線装置１０，３０において秘密鍵Ｋｓ１，Ｋｓ２を生成するとき、後述する方法により、所定の順序に従ってアンテナ部２２０の指向性を順次切換え、またはアンテナ部２２０を無指向性に設定する。

【００４１】

なお、無線装置３０のプロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部２２０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。

【００４２】

図４は、図３に示す指向性設定部２３０の機能ブロック図である。指向性設定部２３０は、制御電圧発生回路２３１と、バラクタダイオード２３２とを含む。制御電圧発生回路２３１は、制御電圧セットＣＬＶ１～ＣＬＶｎ（ｎは自然数）を順次発生し、その発生した制御電圧セットＣＬＶ１～ＣＬＶｎをバラクタダイオード２３２へ順次出力する。バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎに応じて無給電素子であるアンテナ素子２１～２３，２５～２７に装荷される容量を変え、アレーアンテナ２０をオムニアンテナまたは指向性アンテナとして機能させる。すなわち、バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎに応じて無給電素子２１～２３，２５～２７のリアクタンス値を変えることによってアレーアンテナ２０をオムニアンテナまたは指向性アンテナとして機能させる。この場合、制御電圧セットＣＬＶ１～ＣＬＶｎの全てが０Ｖからなるとき、アレーアンテナ２０は、オムニアンテナとして機能する。そして、バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎの複数の異なるセットに応じて、無給電素子２１～２３，２５～２７のリアクタンス値を順次変え、アレーアンテナ２０の指向性を複数個に順次変える。

【００４３】

図５は、図２及び図３に示す鍵一致確認部１７０の概略ブロック図である。鍵一致確認部１７０は、データ発生部１７１と、データ比較部１７２と、結果処理部１７３とを含む。なお、無線装置１０，３０の鍵一致確認部１７０は、同じ構成からなるが、図５におい

ては、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認する動作を説明するために、無線装置３０においてはデータ発生部１７１のみを示す。

【００４４】

データ発生部１７１は、鍵作成部１６０から秘密鍵Ｋｓ１を受けると、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認するための鍵確認用データＤＣＦＭ１を発生し、その発生した鍵確認用データＤＣＦＭ１を送信処理部１２０及びデータ比較部１７２へ出力する。

【００４５】

この場合、データ発生部１７１は、秘密鍵Ｋｓ１から非可逆的な演算及び一方向的な演算等により、鍵確認用データＤＣＦＭ１を発生する。より具体的には、データ発生部１７１は、秘密鍵Ｋｓ１またはＫｓ２のハッシュ値を演算することにより、鍵確認用データＤＣＦＭ１を発生する。

【００４６】

データ比較部１７２は、データ発生部１７１から鍵確認用データＤＣＦＭ１を受け、無線装置３０のデータ発生部１７１で発生された鍵確認用データＤＣＦＭ２を受信処理部１４０から受ける。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１を鍵確認用データＤＣＦＭ２と比較する。データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致するとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。

【００４７】

また、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１７２は、不一致信号ＮＭＴＨを鍵一致化部１９０へ出力し、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００４８】

結果処理部１７３は、データ比較部１７２から一致信号ＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１を鍵記憶部１８０へ記憶する。

【００４９】

図６は、図２及び図３に示す鍵一致化部１９０の概略ブロック図である。鍵一致化部１９０は、擬似シンドローム作成部１９１と、不一致ビット検出部１９２と、鍵不一致訂正部１９３と、データ発生部１９４と、データ比較部１９５と、結果処理部１９６とを含む。

【００５０】

なお、無線装置１０，３０の鍵一致化部１９０は、同じ構成からなるが、図６においては、秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる動作を説明するために、無線装置３０においては擬似シンドローム作成部１９１のみを示す。

【００５１】

擬似シンドローム作成部１９１は、鍵一致確認部１７０のデータ比較部１７２から不一致信号ＮＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１のシンドロームｓ１を演算する。より具体的には、擬似シンドローム作成部１９１は、秘密鍵Ｋｓ１のビットパターンx_1を検出し、ビットパターンx_1に対して検査行列Ｈを乗算してシンドローム$s1 = x_1 H^T$を演算する。そして、擬似シンドローム作成部１９１は、ビットパターンx_1を鍵不一致訂正部１９３へ出力し、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力する。

【００５２】

なお、これらの演算は、ｍｏｄ２の演算であり、H^Tは、検査行列Ｈの転置行列である。

【００５３】

不一致ビット検出部１９２は、擬似シンドローム作成部１９１からシンドロームｓ１を受け、無線装置３０の擬似シンドローム作成部１９１によって演算されたシンドロームｓ

２＝ｘ２ Ｈ^{T} を受信処理部１４０から受ける。そして、不一致ビット検出部１９２は、シンドロームｓ１とシンドロームｓ２との差分ｓ＝ｓ１－ｓ２を演算する。

【００５４】

なお、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンの差分（鍵不一致のビットパターン）をｅ＝ｘ１－ｘ２とすると、ｓ＝ｅＨ^{T} の関係が成立する。ｓ＝０の場合、ｅ＝０となり、秘密鍵Ｋｓ１のビットパターンは、秘密鍵Ｋｓ２のビットパターンに一致する。

【００５５】

不一致ビット検出部１９２は、演算した差分ｓが０でないとき（即ち、ｅ≠０のとき）、鍵不一致のビットパターンの差分ｅを鍵不一致訂正部１９３へ出力する。

【００５６】

鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からビットパターンｘ１を受け、不一致ビット検出部１９２から鍵不一致のビットパターンの差分ｅを受ける。そして、鍵不一致訂正部１９３は、ビットパターンｘ１から鍵不一致のビットパターンの差分ｅを減算することにより相手方の秘密鍵のビットパターンｘ２＝ｘ１－ｅを演算する。

【００５７】

このように、鍵一致化部１９０は、秘密鍵Ｋｓ１，Ｋｓ２の不一致を誤りと見なして誤り訂正の応用により秘密鍵Ｋｓ１，Ｋｓ２の不一致を解消する。

【００５８】

この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるので、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

【００５９】

データ発生部１９４は、一致化後の秘密鍵のビットパターンｘ２＝ｘ１－ｅを鍵不一致訂正部１９３から受けると、ｘ２に基づいて鍵確認用データＤＣＦＭ３を発生させ、その発生させた鍵確認用データＤＣＦＭ３をデータ比較部１９５へ出力する。また、データ発生部１９４は、発生させた鍵確認用データＤＣＦＭ３を送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００６０】

なお、データ発生部１９４は、鍵一致確認部１７０のデータ発生部１７１による鍵確認用データＤＣＦＭ１の発生方法と同じ方法により鍵確認用データＤＣＦＭ３を発生する。

【００６１】

データ比較部１９５は、データ発生部１９４から鍵確認用データＤＣＦＭ３を受け、無線装置３０で発生された鍵確認用データＤＣＦＭ４を受信処理部１４０から受ける。そして、データ比較部１９５は、鍵確認用データＤＣＦＭ３を鍵確認用データＤＣＦＭ４と比較する。

【００６２】

データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に一致するとき、一致信号ＭＴＨを生成して結果処理部１９６へ出力する。

【００６３】

また、データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１９５は、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００６４】

結果処理部１９６は、データ比較部１９５から一致信号ＭＴＨを受けると、鍵不一致訂正部１９３から受けたｘ２＝ｘ１－ｅを鍵記憶部１８０へ記憶する。

【００６５】

このように、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における確認方法と同じ方法によって一致化が施された鍵の一致を確認する。

【００６６】
図７は、受信信号プロファイルＲＳＳＩの概念図である。図３および図４に示した指向性設定部２３０の制御電圧発生回路２３１は、各々が電圧Ｖ１～Ｖ６からなる制御電圧ＣＬＶ１～ＣＬＶｎを順次発生してバラクタダイオード２３２へ出力する。この場合、電圧Ｖ１～Ｖ６は、それぞれ、アンテナ素子２１～２３，２５～２７に装荷される容量を変えるための電圧であり、０～２０Ｖの範囲で変えられる。
【００６７】
バラクタダイオード２３２は、パターンＰ１からなる制御電圧ＣＬＶ１に応じてアレーアンテナ２０の指向性をある１つの指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ１を検出する。
【００６８】
次に、バラクタダイオード２３２は、パターンＰ２からなる制御電圧ＣＬＶ２に応じてアレーアンテナ２０の指向性を別の指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ２を検出する。
【００６９】
以後、同様にして、バラクタダイオード２３２は、それぞれ、パターンＰ３～Ｐｎからなる制御電圧ＣＬＶ３～ＣＬＶｎに応じてアレーアンテナ２０の指向性を順次変える。そして、アレーアンテナ２０は、各々設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ３～ＷＩｎを順次検出する。
【００７０】
そして、プロファイル生成部１５０は、強度ＷＩ１～ＷＩｎからなる強度プロファイルを示す受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。
【００７１】
パターンＰ１～Ｐｎによってアレーアンテナ２０の指向性を複数個に順次切換えて無線装置３０から無線装置１０へデータを送信したとき、無線装置１０のプロファイル生成部１５０が受信信号プロファイルＲＳＳＩを生成する。
【００７２】
鍵作成部１６０は、プロファイル生成部１５０から受信信号プロファイルＲＳＳＩを受け、受信信号プロファイルＲＳＳＩから最大強度ＷＩｍａｘ（＝ＷＩ６）を検出する。そして、鍵作成部１６０は、最大強度ＷＩｍａｘ（＝ＷＩ６）によって受信信号プロファイルＲＳＳＩを規格化し、各強度ＷＩ１～ＷＩｎを多値化する。鍵作成部１６０は、多値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵Ｋｓ１またはＫｓ２を作成する。
【００７３】
図８は、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層およびＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）層のフォーマットを示す図である。物理層は、データを電気信号に変換し、実際の伝送を行なう階層である。そして、物理層は、ＩＥＥＥ８０２．１１ｂおよびＩＥＥＥ８０２．１１ｇの両方に共通なデータフォーマットからなる。また、ＭＡＣ層は、各無線装置間で信頼性の高いデータ伝送を行なう階層である。物理層は、ＰＬＣＰ（Ｐｈｙｓｉｃａｌ　Ｌａｙｅｒ　Ｃｏｎｖｅｒｇｅｎｃｅ　Ｐｒｏｔｏｃｏｌ）プリアンブルと、ＰＬＣＰヘッダとからなる。
【００７４】
ＰＬＣＰプリアンブルは、ＳＹＮＣ（ＳＹＮＣｈｒｏｎｉｚａｔｉｏｎ　ｆｉｅｌｄ）信号と、ＳＦＤ（Ｓｔａｒｔ　Ｆｒａｍｅ　Ｄｅｌｉｍｅｔｅｒ）信号とからなる。また

、ＰＬＣＰヘッダは、ＳＩＧＮＡＬ（ＳＩＧＮＡＬ　ｏｒ　ｄａｔａ　ｒａｔｅ）信号と、ＳＥＲＶＩＣＥ信号と、ＬＥＮＧＴＨ信号と、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｏｄｅ）信号とからなる。

【００７５】

ＳＹＮＣ信号は、１２８ビットのデータ長を有する信号であり、同期の確立に使用される。ＳＦＤ信号は、１６ビットのデータ長を有する信号であり、ＰＬＣＰプリアンブルの終了を示す。

【００７６】

ＳＩＧＮＡＬ信号は、８ビットのデータ長を有する信号であり、ＭＡＣ層のデータ速度を示す。ＳＥＲＶＩＣＥ信号は、８ビットのデータ長を有する信号であり、機能拡張用として予約されている。ＬＥＮＧＴＨ信号は、１６ビットのデータ長を有する信号であり、ＭＡＣ層のデータ長を示す。ＣＲＣ信号は、１６ビットのデータ長を有する信号であり、誤り検出に用いられる。

【００７７】

また、ＭＡＣ層は、ＰＳＤＵ（ＰＬＣＰ　Ｓｅｒｖｉｃｅ　Ｄａｔａ　Ｕｎｉｔ）からなる。そして、ＰＳＤＵは、４８ビット以上のデータ長を有するＭＡＣ層のデータである。

【００７８】

この発明においては、秘密鍵Ｋｓ１，Ｋｓ２を生成する場合、無線装置１０，３０は、所定のデータを物理層に含め、アレーアンテナ２０の指向性を変化させながら送信する。より具体的には、ＳＹＮＣ信号、ＳＦＤ信号、ＳＩＧＮＡＬ信号、ＳＥＲＶＩＣＥ信号、ＬＥＮＧＴＨ信号およびＣＲＣ信号のうち、ＳＹＮＣ信号、ＳＦＤ信号、ＳＩＧＮＡＬ信号およびＳＥＲＶＩＣＥ信号を複数のデータＤ０～Ｄ１１から構成する。そして、複数のデータＤ１～Ｄ１１は、所定のデータを分割したデータである。

【００７９】

データＤ０は、３６ビットのデータ長を有する。また、複数のデータＤ１～Ｄ１１の各々は、１１ビットのデータ長を有する。１１ビットのデータ長に相当する時間長を期間Ｔ０とすると、複数のデータＤ１～Ｄ１１の各々は、３ビットのデータ長に相当する期間Ｔ１と、８ビットのデータ長に相当する期間Ｔ２とに分割される。

【００８０】

秘密鍵Ｋｓ１，Ｋｓ２を生成する場合、データＤ０のデータ長に相当する期間Ｔ３、アレーアンテナ２０をオムニアンテナとして機能させ、データＤ１～Ｄ１１全体のデータ長に相当する期間Ｔ４、アレーアンテナ２０を指向性アンテナとして機能させ、ＬＥＮＧＴＨ信号およびＣＲＣ信号のデータ長に相当する期間Ｔ５、アレーアンテナ２０をオムニアンテナとして機能させて所定のデータを送信する。

【００８１】

そして、期間Ｔ４においてアレーアンテナ２０を指向性アンテナとして機能させる場合、アレーアンテナ２０の指向性が順次切換えられる。より具体的には、複数のデータＤ１～Ｄ１１の各々の期間Ｔ１においてアレーアンテナ２０の指向性が変化され、期間Ｔ２において、その変化された指向性でデータが送信される。従って、図８に示す例においては、アレーアンテナ２０の指向性が１１回変更されて所定のデータが送信される。

【００８２】

所定のデータを受信する場合、所定のデータの送信時と同じように、期間Ｔ３，Ｔ５においてアレーアンテナ２０をオムニアンテナとして機能させ、期間Ｔ４においてアレーアンテナ２０を指向性アンテナとして機能させる。そして、所定のデータの受信時においては、複数のデータＤ１～Ｄ１１の各々の期間Ｔ１においてアレーアンテナ２０の指向性が変化され、その変化された指向性で受信した電波の強度が期間Ｔ２において検出される。従って、図８に示す例においては、所定のデータの受信時においても、アレーアンテナ２０の指向性は、１１回変更される。

【００８３】

なお、期間Ｔ３においてアレーアンテナ２０をオムニアンテナとして機能させるのは、通信の初期においては、ＡＧＣ（Ａｕｔｏ　Ｇａｉｎ　Ｃｏｎｔｒｏｌ）機能を働かせ、データの受信レベルを最適値に調整する必要があるからである。また、期間Ｔ５においてアレーアンテナ２０をオムニアンテナとして機能させるのは、次の理由による。物理層およびＭＡＣ層のデータ受信に誤りが生じると、確認応答（＝ＡＣＫ信号）が返らず、再送状態が続いてしまう。したがって、これを防止するためにＭＡＣ層のデータに関連するＬＥＮＧＴＨ信号および物理層のデータ受信の成否を判定するＣＲＣ信号をオムニアンテナで送受信することにしたものである。

【００８４】

図９は、２つの無線装置１０，３０間でデータを送受信する通常の方法の概念図である。また、図１０は、２つの無線装置１０，３０間におけるデータの再送の概念図である。更に、図１１は、この発明の実施の形態において、２つの無線装置１０，３０間でデータを送受信する方法の概念図である。

【００８５】

通常の方法においては、無線装置１０は、アレーアンテナ２０の指向性をリアクタンス変化パターン（１）に従って順次切換えて所定のデータＤａｔａを無線装置３０へ送信する。そして、無線装置３０は、所定のデータＤａｔａの受信を確認すると、確認応答Ａｃｋを無線装置１０へ送信し、無線装置１０は、アレーアンテナ２０の指向性をリアクタンス変化パターン（１）に従って順次切換えて確認応答Ａｃｋを受信する。その後、無線装置１０は、アレーアンテナ２０の指向性をリアクタンス変化パターン（２）に従って順次切換えて所定のデータＤａｔａを無線装置３０へ送信する。そして、無線装置３０は、無線装置１０から所定のデータＤａｔａを受信する（図９参照）。

【００８６】

しかし、このような通常の方法においては、アレーアンテナ２０の指向性の変更によって図８に示すＳＹＮＣ信号以降のデータを誤って受信した場合、物理層の同期は成立しているが、ＭＡＣ層より上位の層の同期が成立しないため、確認応答Ａｃｋが返送されず、図１０に示すように、アレーアンテナ２０の指向性をリアクタンス変化パターン（１）に従って順次切換えて所定のデータＤａｔａを再送する動作が継続する。その結果、無線装置１０，３０間において双方向の通信ができなくなる。

【００８７】

そこで、この発明においては、図１１に示す方法で所定のデータＤａｔａを送受信する。すなわち、無線装置１０は、アレーアンテナ２０にオムニパターンを設定して所定のデータＤａｔａを無線装置３０へ送信する。つまり、無線装置１０は、アレーアンテナ２０をオムニアンテナとして機能させて所定のデータＤａｔａを無線装置３０へ送信する。

【００８８】

そして、無線装置３０は、無線装置１０からの所定のデータＤａｔａの受信を確認すると、確認応答Ａｃｋを無線装置１０へ送信する。無線装置１０は、アレーアンテナ２０の指向性をリアクタンス変化パターン（１）に従って順次切換えて確認応答Ａｃｋを受信する。その後、無線装置１０は、アレーアンテナ２０の指向性をリアクタンス変化パターン（１）に従って順次切換えて所定のデータＤａｔａを無線装置３０へ送信する。そして、無線装置３０は、無線装置１０から所定のデータＤａｔａを受信する（図１１参照）。

【００８９】

図１１に示す方法においては、無線装置１０は、最初の送信において、通信が確立しているオムニパターンを使用するため、無線装置３０から確認応答Ａｃｋを必ず受信できる。その結果、無線装置１０，３０間における双方向の通信を確保できる。

【００９０】

そして、確認応答Ａｃｋは、図８に示す物理層のフォーマットからなるので、無線装置１０は、アレーアンテナ２０の指向性をリアクタンス変化パターン（１）に従って順次切換えて確認応答Ａｃｋを受信するとき、受信した確認応答Ａｃｋに含まれる複数のデータＤ１～Ｄ１１に対応する複数の電波強度を検出できる。また、無線装置１０は、確認応答

Ａｃｋの受信時におけるリアクタンス変化パターン（１）を使用してアレーアンテナ２０の指向性を順次切換えて所定のデータＤａｔａを無線装置３０へ送信するので、無線装置３０は、無線装置１０において検出された複数の電波強度と同じ複数の電波強度を検出できる。

【００９１】

図１１に示す方法によって所定のデータを無線装置１０，３０間で１回送受信した場合、無線装置１０，３０は、１１個の電波強度からなる強度プロファイルＰＩ１１，ＰＩ２１をそれぞれ検出する。そして、無線装置１０，３０間における所定のデータの送受信をｍ（ｍは自然数）回繰返すことによって、無線装置１０，３０は、ｍ個の強度プロファイルＰＩ１１～ＰＩ１ｍ，ＰＩ２１～ＰＩ２ｍをそれぞれ検出する。

【００９２】

そして、強度プロファイルＰＩ１１～ＰＩ１ｍの全体に含まれる電波強度は、図７に示すｎ個の電波強度ＷＩ１～ＷＩｎに等しい。従って、無線装置１０，３０間における所定のデータの１回の送受信によって、ｎ個の電波強度ＷＩ１～ＷＩｎのうちの１１個の電波強度ＷＩ（ｉ）～ＷＩ（ｉ＋１０）（ｉ＝１～ｎ－１０）が検出される。

【００９３】

つまり、この発明においては、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層に所定のデータＤａｔａを含めて無線装置１０，３０間で送受信することをｍ回繰り返すことによってｎ個の電波強度ＷＩ１～ＷＩｎが検出され、その検出されたｎ個の電波強度ＷＩ１～ＷＩｎに基づいて秘密鍵Ｋｓ１，Ｋｓ２が生成される。

【００９４】

図１２は、図１に示す２つの無線装置１０，３０間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置３０の送信処理部１２０は、ｋ＝１を設定する（ステップＳ１）。そして、指向性設定部２３０は、アレーアンテナ２０をオムニアンテナとして機能させ、所定のデータＤａｔａを無線装置１０へ送信する（ステップＳ２）。

【００９５】

続いて、無線装置１０のアンテナ部１３０は、所定のデータＤａｔａを受信し（ステップＳ３）、その受信した所定のデータＤａｔａを受信処理部１４０へ出力する。そして、受信処理部１４０は、所定のデータＤａｔａの受信を確認すると、送信処理部１２０は、確認応答（Ａｃｋ信号）をアンテナ部１３０から無線装置３０へ送信する（ステップＳ４）。

【００９６】

無線装置３０の指向性設定部２３０は、アンテナ部２２０をオムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させ、アンテナ部２２０は、確認応答（Ａｃｋ信号）を受信する（ステップＳ５）。すなわち、アレーアンテナ２０は、図８に示すデータＤ０をオムニアンテナとして受信し、指向性をパターンＰｋにより１１個に変化させながらデータＤ１～Ｄ１１を受信し、更に、ＬＥＮＧＴＨ信号およびＣＲＣ信号をオムニアンテナとして受信する。

【００９７】

そして、アンテナ部２２０は、受信した複数のデータＤ１～Ｄ１１に対応する複数の電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ部部２２０からの複数の電波の強度プロファイルＰＩ１ｋを検出する（ステップＳ６）。

【００９８】

次に、無線装置３０の信号発生部１１０は、所定のデータを発生して送信処理部１２０へ出力し、送信処理部１２０は、所定のデータを物理層のデータＤ１～Ｄ１１に割り当て、オムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させたアンテナ部２２０を介して無線装置１０へ所定のデータを送信する（ステップＳ７）。すなわち、アンテナ部２２０は、図８に示すデータＤ０をオムニアンテナとして送信し、指向性をパ

ターンＰｋにより１１個に変化させながらデータＤ１～Ｄ１１を送信し、更に、ＬＥＮＧＴＨ信号およびＣＲＣ信号をオムニアンテナとして送信する。

【００９９】

無線装置１０において、アンテナ部１３０は、無線装置３０から所定のデータを受信する。（ステップＳ８）。そして、アンテナ部１３０は、受信した複数のデータＤ１～Ｄ１１に対応する複数の電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ部部１３０からの複数の電波の強度プロファイルＰＩ２ｋを検出する（ステップＳ９）。

【０１００】

その後、無線装置３０の送信処理部１２０は、ｋ＝ｋ＋１を設定し（ステップＳ１０）、ｋ＝ｍであるか否かを判定する（ステップＳ１１）。そして、ｋ＝ｍでないとき、ステップＳ２～Ｓ１１が繰返し実行される。即ち、アレーアンテナ２０の指向性パターンがパターンＰ１～Ｐｍによってｍ個に変えられて、無線装置１０のアンテナ部１３０と無線装置３０のアンテナ部２２０との間で所定のデータを構成する電波が送受信され、強度プロファイルＩ１１～Ｉ１ｍ及びＩ２１～Ｉ２ｍが検出されるまで、ステップＳ２～Ｓ１１が繰返し実行される。

【０１０１】

ステップＳ１１において、ｋ＝ｍであると判定されると、無線装置３０において、プロファイル生成部１５０は、強度プロファイルＩ１１～Ｉ１ｍに含まれる強度Ｉ１１～Ｉ１ｎから受信信号プロファイルＲＳＳＩ１を作成して鍵作成部１６０へ出力する。

【０１０２】

鍵作成部１６０は、受信信号プロファイルＲＳＳＩ１から最大強度ＷＩｍａｘ１を検出し、その検出した最大強度ＷＩｍａｘ１によって受信信号プロファイルＲＳＳＩ１を規格化し、強度Ｉ１１～Ｉ１ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ２を生成する（ステップＳ１２）。

【０１０３】

また、無線装置１０のプロファイル生成部１５０は、強度プロファイルＩ２１～Ｉ２ｍに含まれる強度Ｉ２１～Ｉ２ｎから受信信号プロファイルＲＳＳＩ２を作成して鍵作成部１６０へ出力する。鍵作成部１６０は、受信信号プロファイルＲＳＳＩ２から最大強度ＷＩｍａｘ２を検出し、その検出した最大強度ＷＩｍａｘ２によって受信信号プロファイルＲＳＳＩ２を規格化し、強度Ｉ２１～Ｉ２ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ１を生成する（ステップＳ１３）。

【０１０４】

次に、ステップＳ１４において鍵一致の確認が行なわれる。即ち、無線装置１０において、鍵作成部１６０は、秘密鍵Ｋｓ１を鍵一致確認部１７０へ出力する。鍵一致確認部１７０のデータ発生部１７１は、上述した方法によって鍵確認用データＤＣＦＭ１を発生して送信処理部１２０及びデータ比較部１７２へ出力する。送信処理部１２０は、鍵確認用データＤＣＦＭ１に変調等の処理を施し、アンテナ部１３０を介して無線装置３０へ鍵確認用データＤＣＦＭ１を送信する。

【０１０５】

そして、アンテナ部１３０は、無線装置３０において発生された鍵確認用データＤＣＦＭ２を無線装置３０から受信し、その受信した鍵確認用データＤＣＦＭ２を受信処理部１４０へ出力する。受信処理部１４０は、鍵確認用データＤＣＦＭ２に所定の処理を施し、鍵一致確認部１７０のデータ比較部１７２へ鍵確認用データＤＣＦＭ２を出力する。

【０１０６】

データ比較部１７２は、データ発生部１７１からの鍵確認用データＤＣＦＭ１を受信処理部１４０からの鍵確認用データＤＣＦＭ２と比較する。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致しているとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。結果処理部１７３は、一致信号ＭＴＨに応じて、鍵作成部１６０からの秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。

【０１０７】
一方、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、データ比較部１７２は、不一致信号ＮＭＴＨを生成して送信処理部１２０及び鍵一致化部１９０へ出力する。送信処理部１２０は、不一致信号ＮＭＴＨをアンテナ部１３０を介して無線装置３０へ送信する。そして、無線装置３０は、無線装置１０において秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたことを検知する。
【０１０８】
これにより、無線装置１０における鍵一致の確認が終了する（ステップＳ１４）。
【０１０９】
無線装置３０においても、無線装置１０と同じ動作によって鍵一致の確認が行なわれる（ステップＳ１５）。
【０１１０】
ステップＳ１４において、秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたとき、無線装置１０において、鍵一致化部１９０の擬似シンドローム作成部１９１は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受ける。そして、擬似シンドローム作成部１９１は、不一致信号ＮＭＴＨに応じて、鍵作成部１６０から受けた秘密鍵Ｋｓ１のビットパターンx_1を検出し、その検出したビットパターンx_1のシンドローム$s1 = x_1 H^T$を演算する。
【０１１１】
擬似シンドローム作成部１９１は、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力し、ビットパターンx_1を鍵不一致訂正部１９３へ出力する。
【０１１２】
一方、無線装置３０は、ステップＳ１１において無線装置１０から不一致信号ＮＭＴＨを受信し、その受信した不一致信号ＮＭＴＨに応じて、シンドローム$s2 = x_2 H^T$を演算して無線装置１０へ送信する。
【０１１３】
無線装置１０のアンテナ部１３０は、無線装置３０からシンドローム$s2 = x_2 H^T$を受信して受信処理部１４０へ出力する。受信処理部１４０は、シンドローム$s2 = x_2 H^T$に対して所定の処理を施し、シンドローム$s2 = x_2 H^T$を鍵一致化部１９０へ出力する。
【０１１４】
鍵一致化部１９０の不一致ビット検出部１９２は、受信処理部１４０から無線装置３０において作成されたシンドローム$s2 = x_2 H^T$を受ける。そして、不一致ビット検出部１９２は、無線装置１０で作成されたシンドローム$s1 = x_1 H^T$と無線装置３０において作成されたシンドローム$s2 = x_2 H^T$との差分$s = s1 - s2$を演算する。
【０１１５】
その後、不一致ビット検出部１９２は、$s \neq 0$であることを確認し、鍵不一致のビットパターンの差分$e = x_1 - x_2$を$s = e H^T$に基づいて演算し、その演算した鍵不一致のビットパターンの差分ｅを鍵不一致訂正部１９３へ出力する。
【０１１６】
鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からのビットパターンx_1と、不一致ビット検出部１９２からの鍵不一致のビットパターンｅとに基づいて、無線装置３０において作成された秘密鍵Ｋｓ２のビットパターン$x_2 = x_1 - e$を演算する。
【０１１７】
そして、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における鍵一致確認の動作と同じ動作によって、一致化された鍵$x_2 = x_1 - e$の一致を確認する。
【０１１８】
これにより、鍵不一致対策が終了する（ステップＳ１６）。
【０１１９】
無線装置３０においても、無線装置１０と同じ動作によって鍵不一致対策が行なわれる

（ステップＳ１７）。

【０１２０】

ステップＳ１４において、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することが確認されたとき、またはステップＳ１６において鍵不一致対策がなされたとき、暗号部２００は、鍵記憶部１８０から秘密鍵Ｋｓ１を読出して送信データを暗号化し、暗号化した送信データを送信処理部１２０へ出力する。そして、送信処理部１２０は、暗号化された送信データに変調等を施し、アンテナ部１３０を介して暗号化された送信データを無線装置３０へ送信する。

【０１２１】

また、アンテナ部１３０は、暗号化された送信データを無線装置３０から受信し、その受信した暗号化された送信データを受信処理部１４０へ出力する。受信処理部１４０は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部２１０へ出力する。

【０１２２】

復号部２１０は、受信処理部１４０からの暗号化された送信データを復号して受信データを取得する。

【０１２３】

これにより、秘密鍵Ｋｓ１による暗号・復号が終了する（ステップＳ１８）。

【０１２４】

無線装置３０においても、無線装置１０と同じ動作によって秘密鍵Ｋｓ２による暗号・復号が行なわれる（ステップＳ１９）。そして、一連の動作が終了する。

【０１２５】

上述したステップＳ２～４に示す動作は、アレーアンテナ２０をオムニアンテナとして機能させて無線装置１０と無線装置３０との間で通信を確立する動作である。また、ステップＳ４～Ｓ６に示す動作は、無線装置３０において受信信号プロファイルＲＳＳＩ１を生成するための電波を無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ送信し、かつ、無線装置３０において電波の強度プロファイルＰＩ１ｋを検出する動作であり、ステップＳ７～Ｓ９に示す動作は、無線装置１０において受信信号プロファイルＲＳＳＩ２を生成するための電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、かつ、無線装置１０において電波の強度プロファイルＰＩ２ｋを検出する動作である。そして、所定のデータを構成する電波の無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０への送信及び所定のデータを構成する電波の無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１への送信は、アレーアンテナ２０の指向性をパターンＰｋに従って変えながら交互に行なわれる。つまり、所定のデータを構成する電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で時分割通信により送受信される。

【０１２６】

従って、アレーアンテナ２０の指向性をパターンＰｋに従って変えながら無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ所定のデータを構成する電波を送信し、無線装置３０において電波の強度プロファイルＰＩ１ｋを検出した直後に、同じ所定のデータを構成する電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、無線装置１０において電波の強度プロファイルＰＩ２ｋを検出することができる。その結果、無線装置１０，３０間において同じ伝送路特性を確保して所定のデータを構成する電波を無線装置１０；３０間で送受信でき、電波の可逆性により電波の強度Ｉ１１～Ｉ１ｎをそれぞれ電波の強度Ｉ２１～Ｉ２ｎに一致させることができる。そして、無線装置１０において作成される秘密鍵Ｋｓ１を無線装置３０において作成される秘密鍵Ｋｓ２に容易に一致させることができる。

【０１２７】

また、所定のデータを構成する電波は、無線装置１０，３０間で時分割通信により送受信されるので、電波の干渉を抑制して１つのアレーアンテナ２０を介して所定のデータを

構成する電波を無線装置１０，３０間で送受信できる。

【０１２８】

更に、所定のデータは、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂおよびＩＥＥＥ８０２．１１ｇに共通な物理層に含めて無線装置１０，３０間で送受信されるので、通信プロトコルがＩＥＥＥ８０２．１１ｂからＩＥＥＥ８０２．１１ｇへ変化してもデータフォーマットを変えずに秘密鍵Ｋｓ１，Ｋｓ２を生成できる。

【０１２９】

更に、無線装置３０は、無線装置１０からの確認応答（Ａｃｋ信号）の受信時および所定のデータの無線装置１０への送信時、同じパターンＰｋによってアレーアンテナ２０の指向性を順次変更する（ステップＳ５，Ｓ７参照）。そして、同じパターンＰｋによってアレーアンテナ２０の指向性を順次変更して無線装置１０から確認応答（Ａｃｋ信号）を受信する動作（ステップＳ５）および所定のデータを無線装置１０へ送信する動作（ステップＳ７）は、ｋ＝ｍになるまで繰返し実行されるので、ステップＳ５，Ｓ７において、パターンＰｋに従ってアレーアンテナ２０の指向性を順次変更することは、アレーアンテナ２０の指向性を更新して無線装置１０から確認応答（Ａｃｋ信号）を受信し、その更新した指向性を維持して所定のデータを無線装置１０へ送信することに相当する。

【０１３０】

このように、図１１に示す方法によって所定のデータを無線装置１０，３０間で送受信することによって所定のデータの再送が繰返されるのを防止し、無線装置１０，３０間における双方向の通信を確保できる。すなわち、無線装置１０，３０において同じ秘密鍵Ｋｓ１，Ｋｓ２を安定して作成できる。

【０１３１】

更に、アレーアンテナ２０の指向性をパターンＰｋに従って変えながら無線装置１０，３０間で所定のデータを構成する電波を送受信し、秘密鍵Ｋｓ１，Ｋｓ２を作成するための受信信号プロファイルＲＳＳＩ１，ＲＳＳＩ２を生成するので、図１に示すようにアレーアンテナ２０を装着した無線装置３０の近傍に盗聴装置５０が配置されていても、盗聴装置５０による秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０１３２】

即ち、盗聴装置５０は、アンテナ１１及びアレーアンテナ２０から送信された電波をアンテナ５１を介して受信するが、アレーアンテナ２０は指向性をパターンＰｋに従って変えながら電波を送受信するので、アンテナ１１とアレーアンテナ２０との間で送受信される電波は、アンテナ１１またはアレーアンテナ２０とアンテナ５１との間で送受信される電波と異なり、盗聴装置５０は、無線装置３０が送受信する電波と同じ電波を送受信できず、電波の強度プロファイルＰＩ１ｋと同じ強度プロファイルを得ることができない。その結果、盗聴装置５０は、秘密鍵Ｋｓ１，Ｋｓ２を盗聴することができない。

【０１３３】

従って、この発明においては、電気的に指向性を切換え可能なアレーアンテナ２０を盗聴装置５０の近傍に配置された無線装置３０に装着することを特徴とする。

【０１３４】

更に、鍵確認用データＤＣＦＭ１～４は、秘密鍵Ｋｓ１，Ｋｓ２に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データＤＣＦＭ１～４が盗聴されても秘密鍵Ｋｓ１，Ｋｓ２が解読される危険性を極めて低くできる。

【０１３５】

更に、シンドロームｓ１，ｓ２は、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンを示す鍵x_1，x_2に検査行列Ｈの転置行列H^Tを乗算して得られるので、シンドロームｓ１，ｓ２が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

【０１３６】

なお、無線装置１０，３０間で通信を行なう動作は、実際には、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）によって行なわれ、無線装置１０に搭載されたＣ

ＰＵは、図１２に示す各ステップＳ３，Ｓ４，Ｓ８，Ｓ９，Ｓ１３，Ｓ１４，Ｓ１６，Ｓ１８を備えるプログラムをＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）から読出し、無線装置３０に搭載されたＣＰＵは、図１２に示す各ステップＳ１，Ｓ２，Ｓ５，Ｓ６，Ｓ７，Ｓ１０，Ｓ１１，Ｓ１２，Ｓ１５，Ｓ１７，Ｓ１９を備えるプログラムをＲＯＭから読出し、無線装置１０，３０に搭載された２つのＣＰＵは、その読出したプログラムを実行して図１２に示すフローチャートに従って無線装置１０，３０間で通信を行なう。

【０１３７】

従って、ＲＯＭは、無線装置１０，３０間で通信を行なう動作をコンピュータ（ＣＰＵ）に実行させるためのプログラムを記録したコンピュータ（ＣＰＵ）読取り可能な記録媒体に相当する。

【０１３８】

そして、図１２に示す各ステップを備えるプログラムは、アレーアンテナ２０の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置１０，３０間における通信をコンピュータ（ＣＰＵ）に実行させるプログラムである。

【０１３９】

上記においては、電気的に指向性を切換え可能なアレーアンテナ２０を無線装置３０のみに装着すると説明したが、この発明においては、アレーアンテナ２０は、無線装置１０及び３０の両方に装着されてもよい。

【０１４０】

即ち、この発明においては、アレーアンテナ２０は、２つの無線装置１０，３０のうち、少なくとも一方の無線装置に装着されていればよい。そして、アレーアンテナ２０を装着した無線装置は、好ましくは、盗聴装置５０の近傍に配置される。

【０１４１】

また、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、無線装置１０，３０間の通信環境に応じて決定されてもよい。即ち、無線装置１０，３０間の通信環境が盗聴し易い環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、無線装置１０，３０間の通信環境が盗聴しにくい環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

【０１４２】

更に、定期的に秘密鍵Ｋｓ１，Ｋｓ２の鍵長を変えるようにしてもよい。

【０１４３】

更に、無線装置１０，３０間で送受信する情報の機密性に応じて秘密鍵Ｋｓ１、Ｋｓ２の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

【０１４４】

そして、この鍵長は、アレーアンテナ２０の指向性を変化させる個数、即ち、制御電圧ＣＬＶ１～ＣＬＶｎの個数により制御される。秘密鍵Ｋｓ１，Ｋｓ２は、検出された電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数からなるビットパターンを有し、電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数は、アレーアンテナ２０の指向性を変化させる個数に等しいからである。つまり、制御電圧ＣＬＶ１～ＣＬＶｎの個数により秘密鍵Ｋｓ１，Ｋｓ２の鍵長を制御できる。

【０１４５】

このように、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、電気的に指向性を切換え可能なアレーアンテナ２０の指向性を変化させる個数によって決定される。

【０１４６】

更に、上記においては、２つの無線装置間において秘密鍵を生成する場合、即ち、１つの無線装置が１つの無線装置と通信する場合について説明したが、この発明は、これに限らず、１つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、１つの無線装置は、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変え

て秘密鍵を生成する。１つの無線装置は、アレーアンテナ２０の指向性の切換パターンを１つに固定して複数の無線装置との間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって１つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

【０１４７】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【産業上の利用可能性】

【０１４８】

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。

【図面の簡単な説明】

【０１４９】

【図１】この発明の実施の形態による無線通信システムの概略図である。

【図２】図１に示す一方の無線装置の内部構成を示す概略ブロック図である。

【図３】図１に示す他方の無線装置の内部構成を示す概略ブロック図である。

【図４】図３に示す指向性設定部の機能ブロック図である。

【図５】図２及び図３に示す鍵一致確認部の概略ブロック図である。

【図６】図２及び図３に示す鍵一致化部の概略ブロック図である。

【図７】受信信号プロファイルＲＳＳＩの概念図である。

【図８】所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層およびＭＡＣ層のフォーマットを示す図である。

【図９】２つの無線装置間でデータを送受信する通常の方法の概念図である。

【図１０】２つの無線装置間におけるデータの再送の概念図である。

【図１１】この発明の実施の形態において、２つの無線装置間でデータを送受信する方法の概念図である。

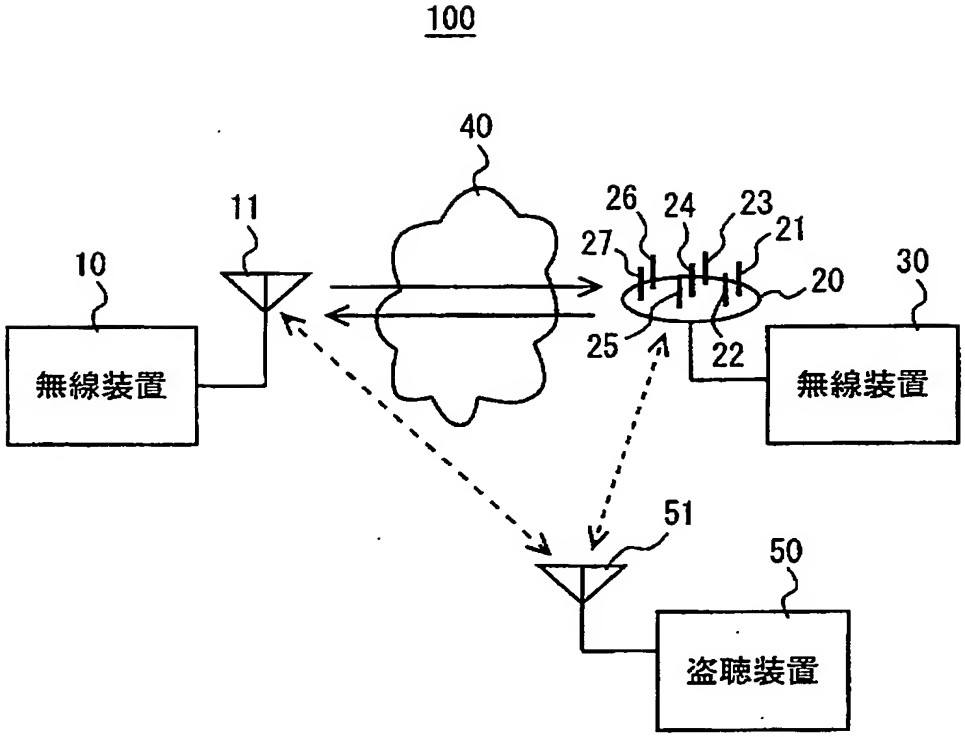
【図１２】図１に示す２つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

【符号の説明】

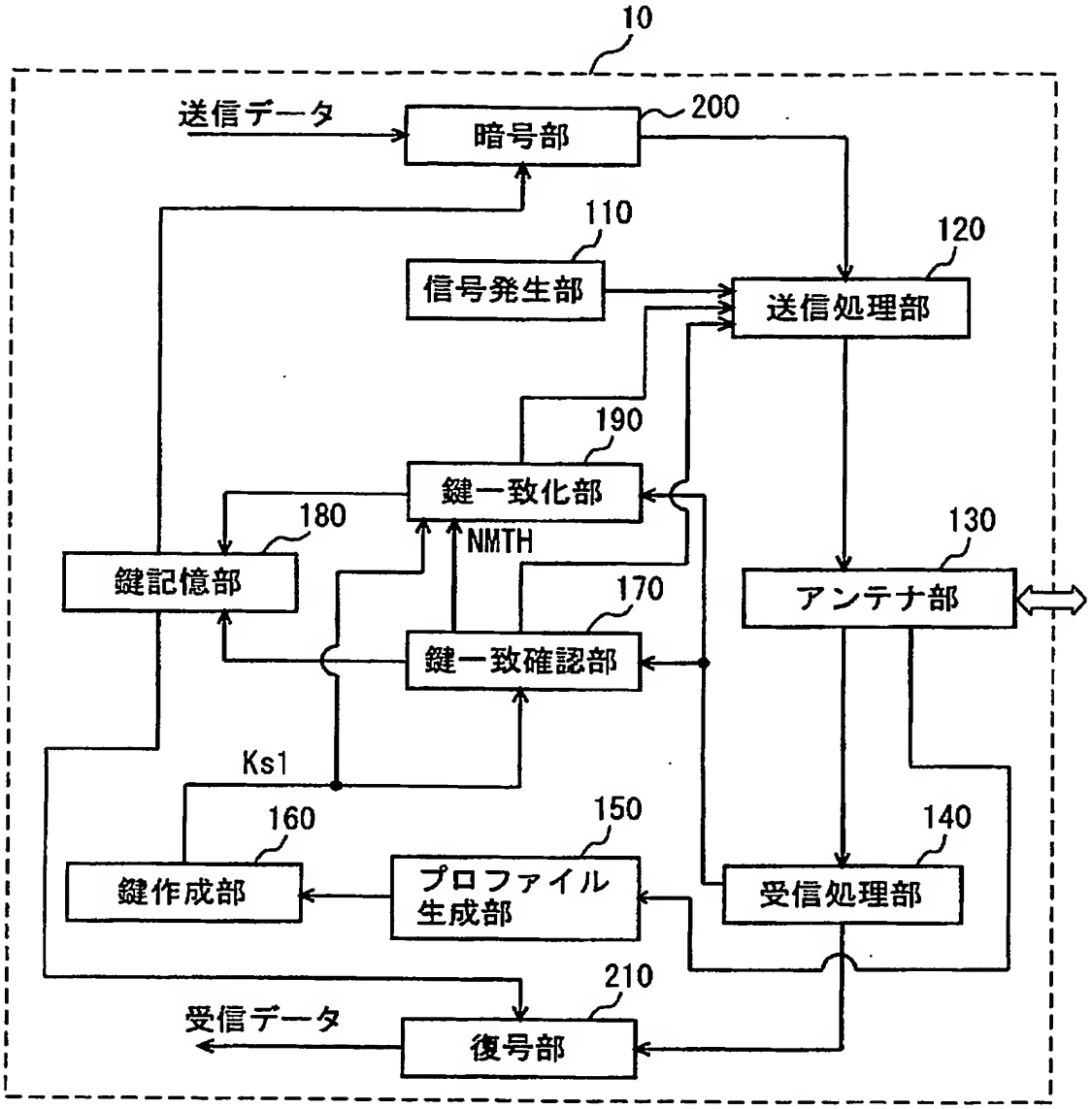
【０１５０】

１０，３０　無線装置、１１，５１　アンテナ、２０　アレーアンテナ、２１～２７　アンテナ素子、４０　中間物、５０　盗聴装置、１００　無線通信システム、１１０　信号発生部、１２０　送信処理部、１３０，２２０　アンテナ部、１４０　受信処理部、１５０　プロファイル生成部、１６０　鍵作成部、１７０　鍵一致確認部、１７１，１９４　データ発生部、１７２，１９５　データ比較部、１７３，１９６　結果処理部、１８０　鍵記憶部、１９０　鍵一致化部、１９１　擬似シンドローム作成部、１９２　不一致ビット検出部、１９３　鍵不一致訂正部、２００　暗号部、２１０　復号部、２３０　指向性設定部、２３１　制御電圧発生回路、２３２　バラクタダイオード。

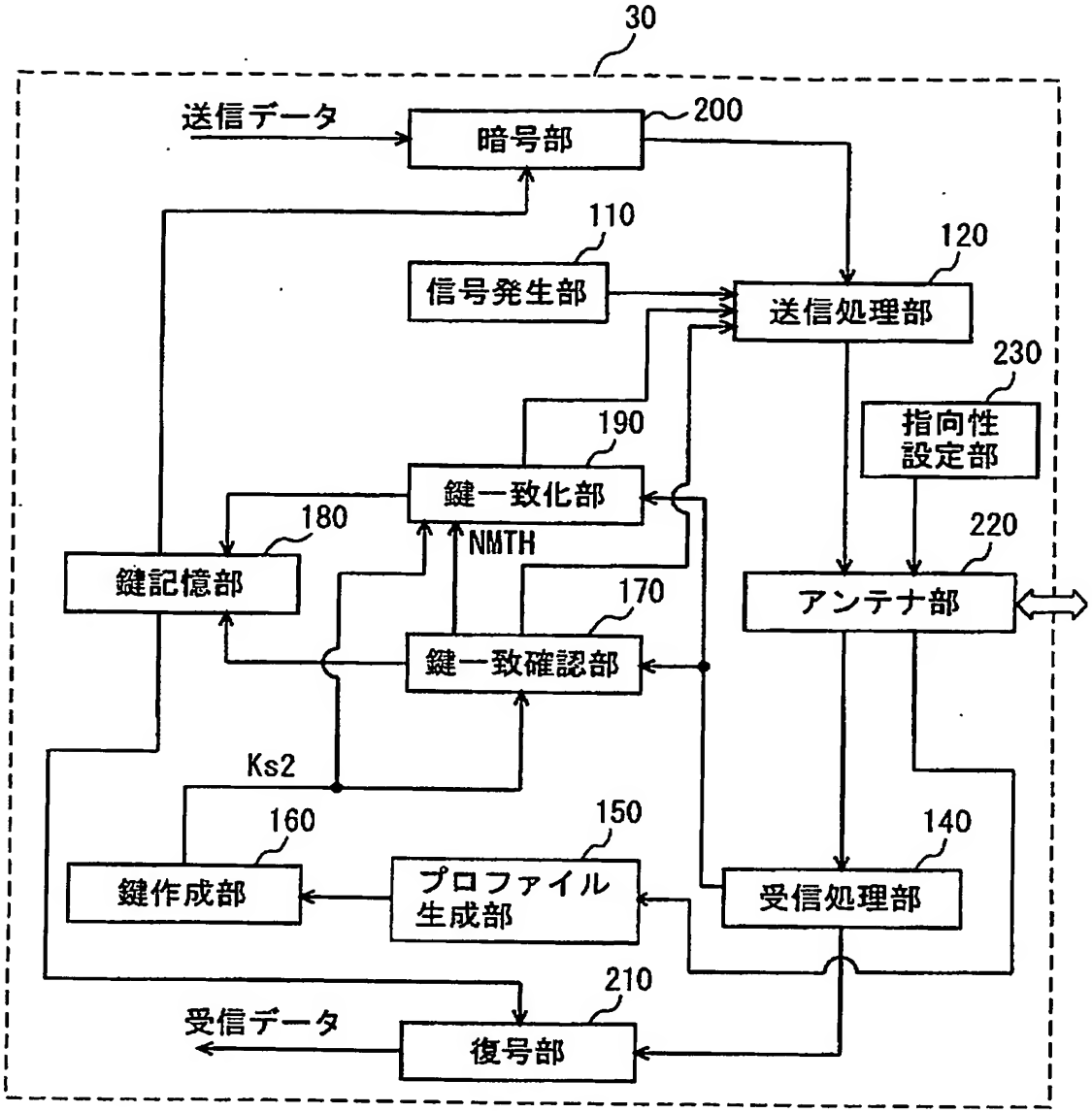
【書類名】図面
【図１】



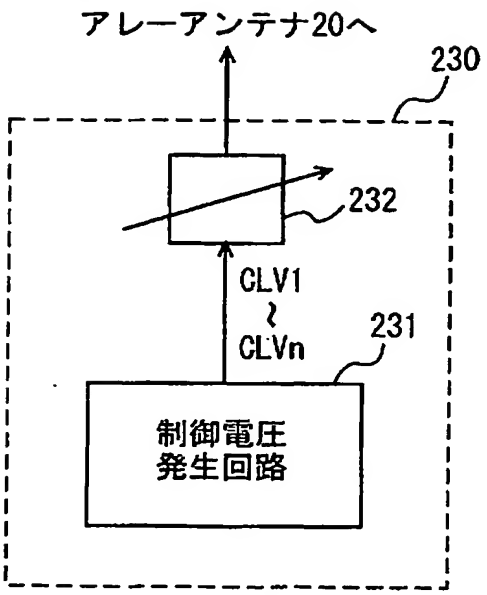
【図２】


10
送信データ
暗号部
200
110
信号発生部
120
送信処理部
190
鍵一致化部
180
NMTH
鍵記憶部
130
アンテナ部
170
鍵一致確認部
Ks1
160
150
140
鍵作成部
プロファイル
生成部
受信処理部
210
受信データ
復号部

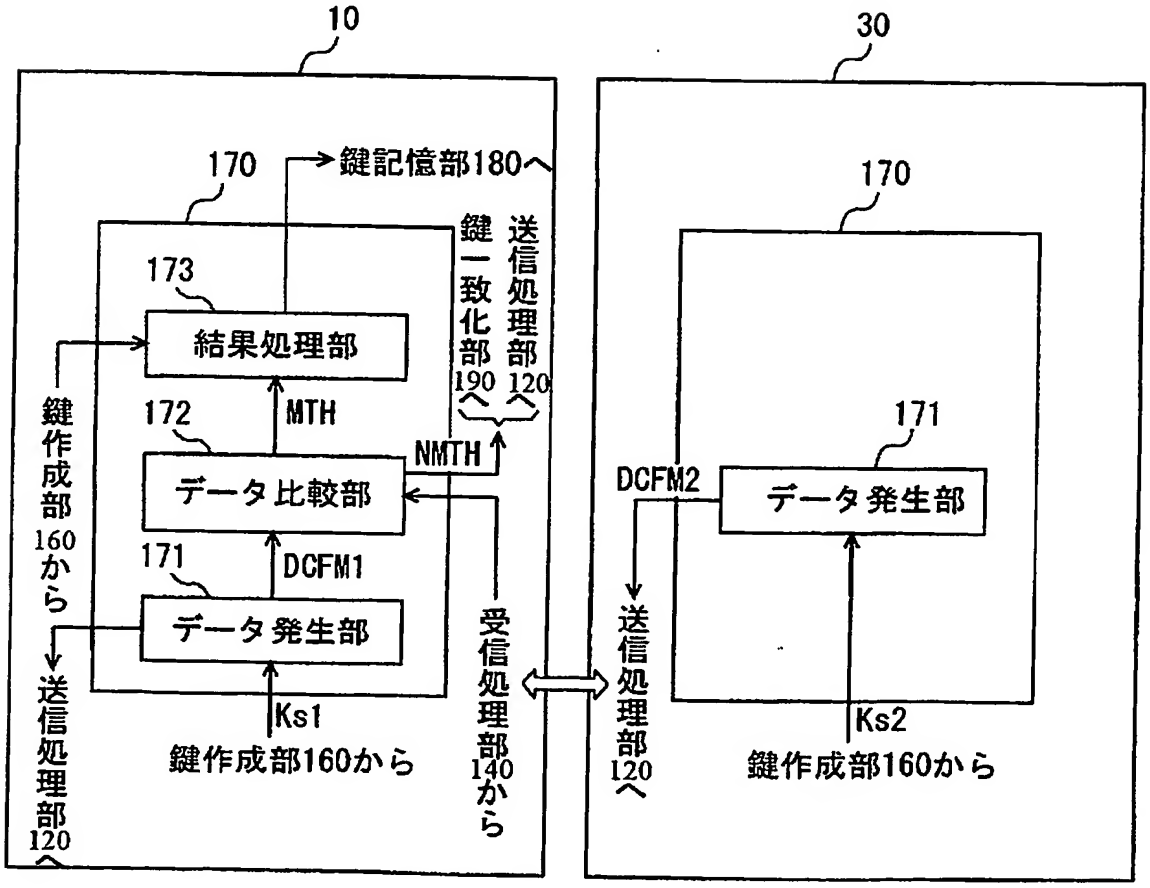
【図３】


30
送信データ
暗号部
200
110
信号発生部
120
送信処理部
230
指向性
設定部
190
鍵一致化部
180
NMTH
220
鍵記憶部
アンテナ部
170
鍵一致確認部
Ks2
160
150
140
鍵作成部
プロファイル
生成部
受信処理部
210
受信データ
復号部

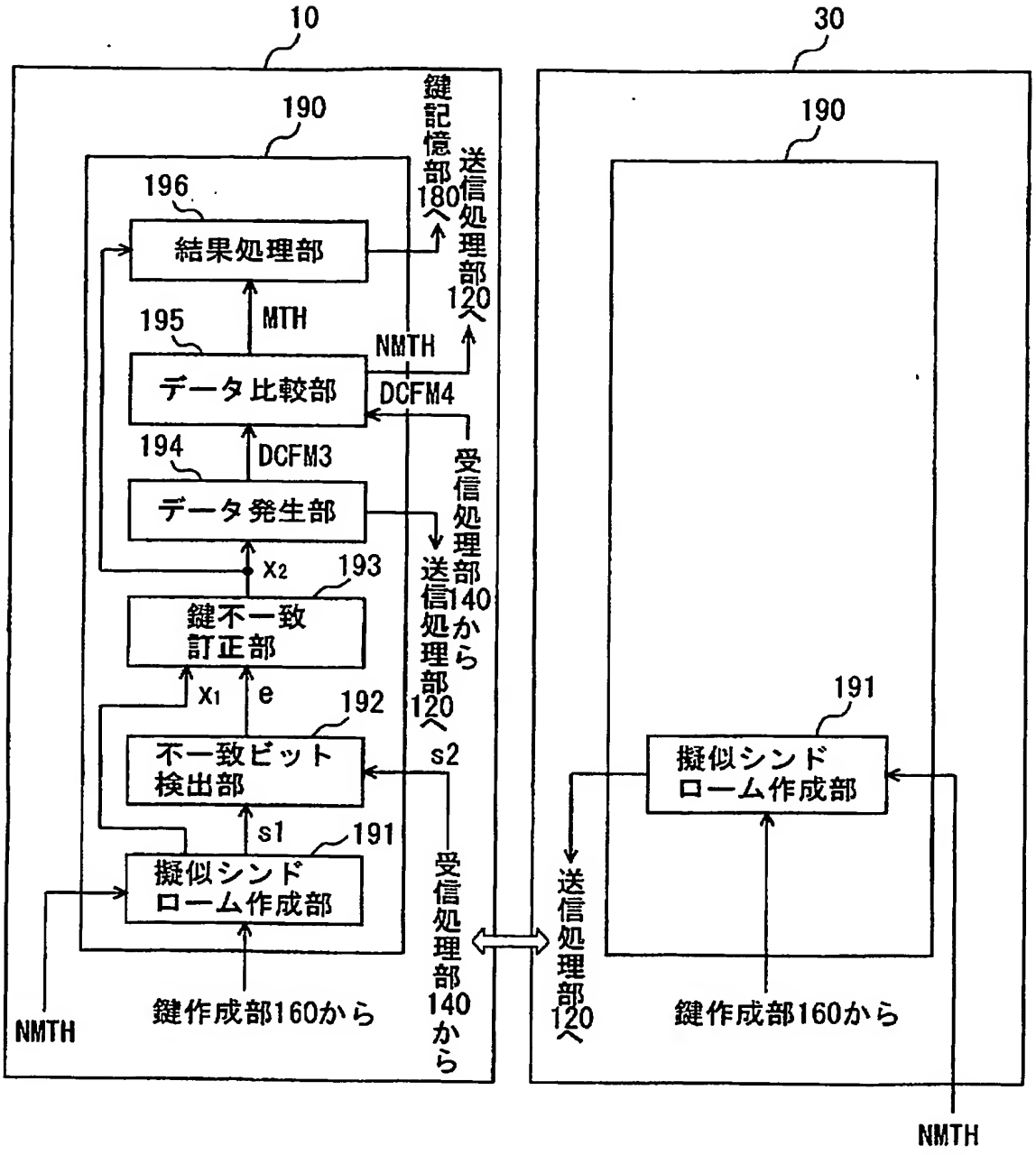
【図４】


アレーアンテナ20へ
230
232
CLV1
～
CLVn
231
制御電圧
発生回路

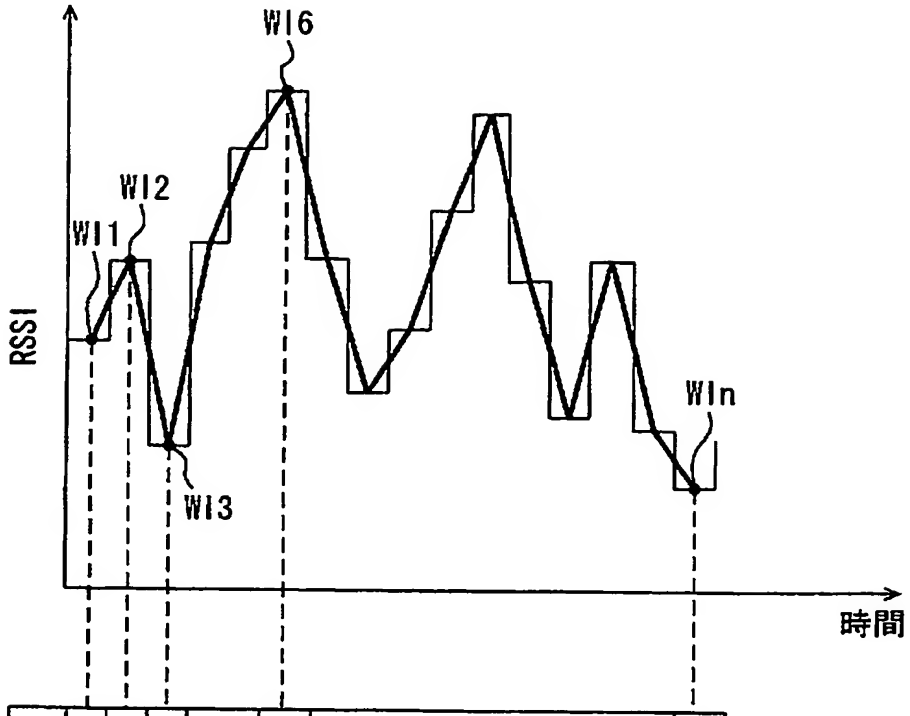
【図５】


10
30
170
鍵記憶部180へ
鍵一致化部190へ
送信処理部120へ
173
結果処理部
鍵作成部160から
送信処理部120へ
172
MTH
NMTH
データ比較部
171
DCFM1
データ発生部
Ks1
鍵作成部160から
受信処理部140から
170
171
DCFM2
データ発生部
送信処理部120へ
Ks2
鍵作成部160から

【図６】

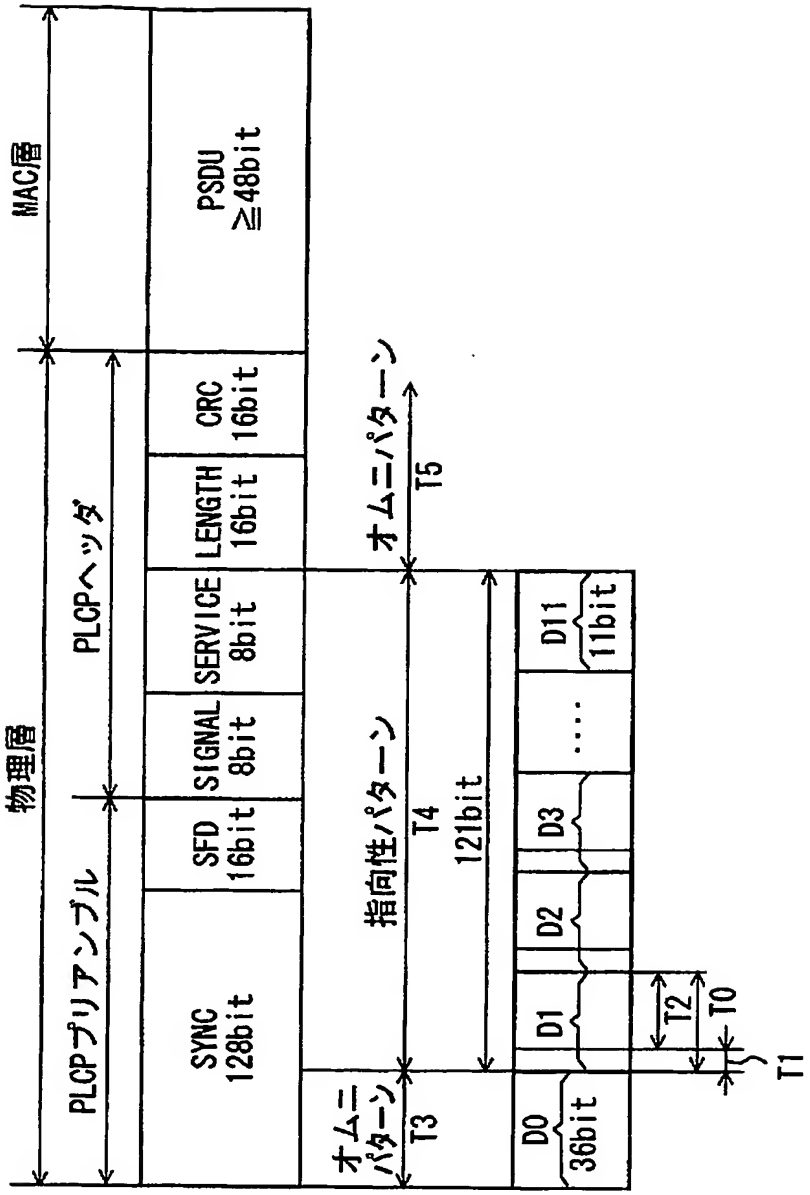

10
30
190
190
190
196
結果処理部
195
MTH
データ比較部
194
DCFM3
データ発生部
193
鍵不一致
訂正部
192
不一致ビット
検出部
191
擬似シンド
ローム作成部
191
擬似シンド
ローム作成部
鍵記憶部
180へ
送信処理部
120へ
NMTH
DCFM4
受信処理部
140から
送信処理部
120へ
s2
受信処理部
140
から
s1
X2
X1
e
NMTH
鍵作成部160から
送信処理部
120へ
鍵作成部160から
NMTH

【図７】

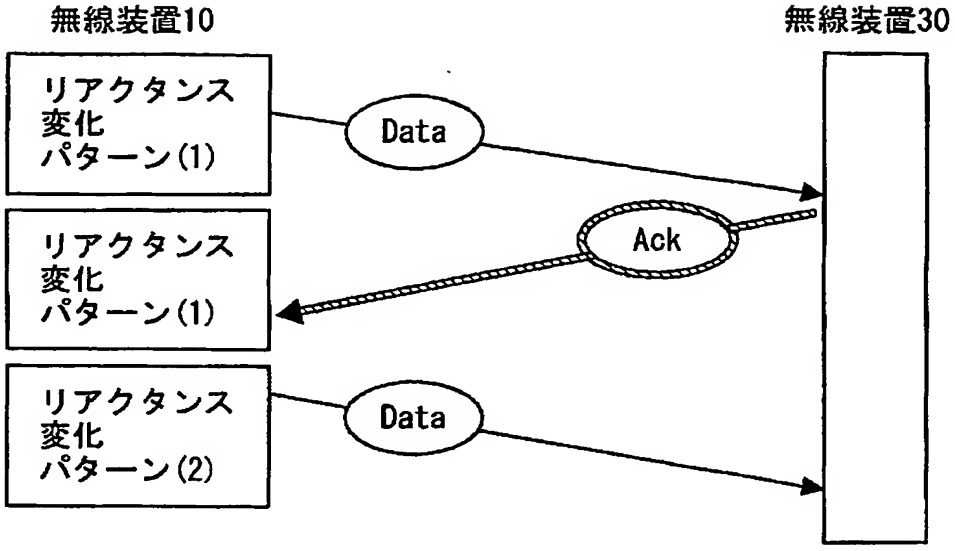


	P1	P2	P3	..	P6	.....	Pn
V1	0	1	2		0		0
V2	0	0	0		1		1
V3	1	0	0		0		0
V4	0	0	0	..	0	.....	2
V5	0	0	0		0		0
V6	0	0	0		0		1

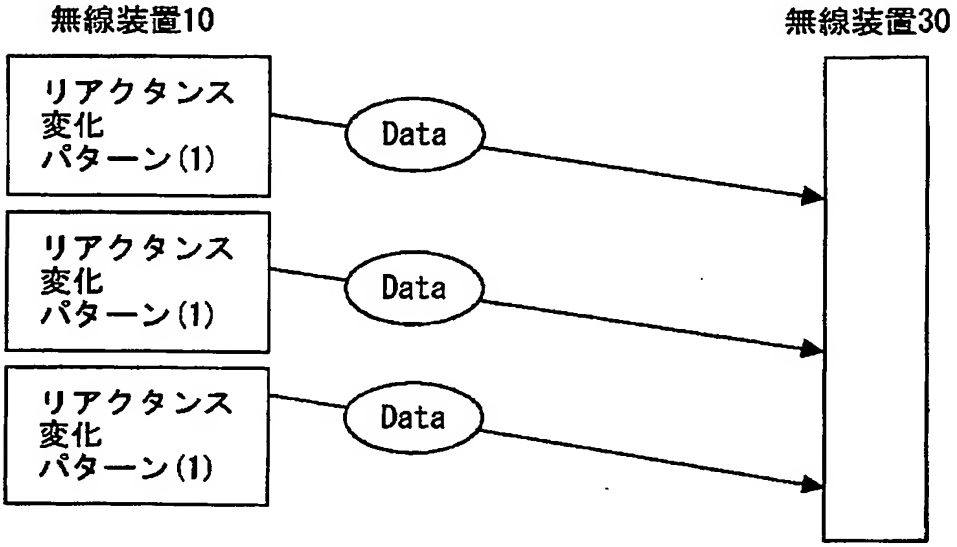
【図８】


物理層
MAC層
PLCPプリアンブル
PLCPヘッダ
SYNC 128bit
SFD 16bit
SIGNAL 8bit
SERVICE 8bit
LENGTH 16bit
CRC 16bit
PSDU ≧48bit
オムニパターン T3
指向性パターン T4 121bit
オムニパターン T5
D0 36bit
D1
D2
D3
D11 11bit
T0
T1
T2

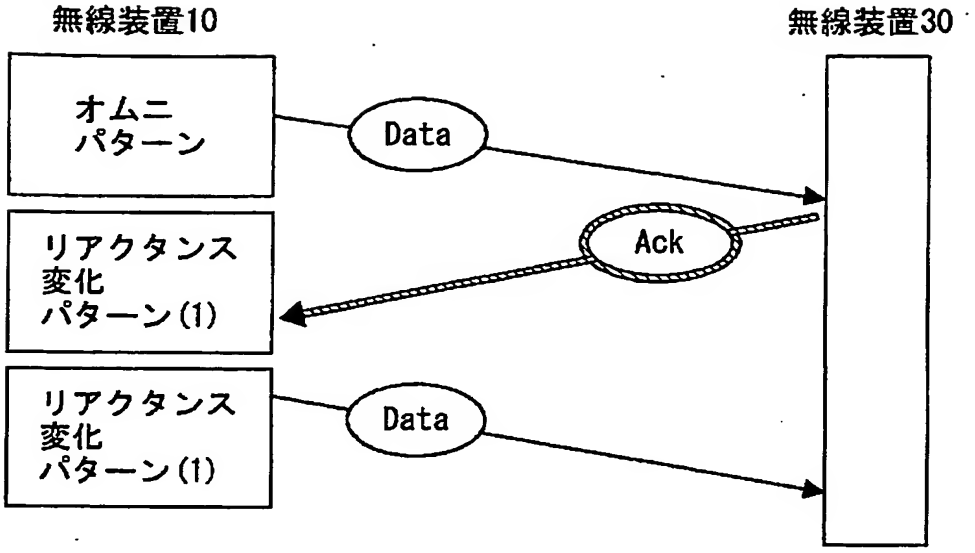
【図９】


無線装置10
無線装置30
リアクタンス変化パターン(1)
Data
リアクタンス変化パターン(1)
Ack
リアクタンス変化パターン(2)
Data

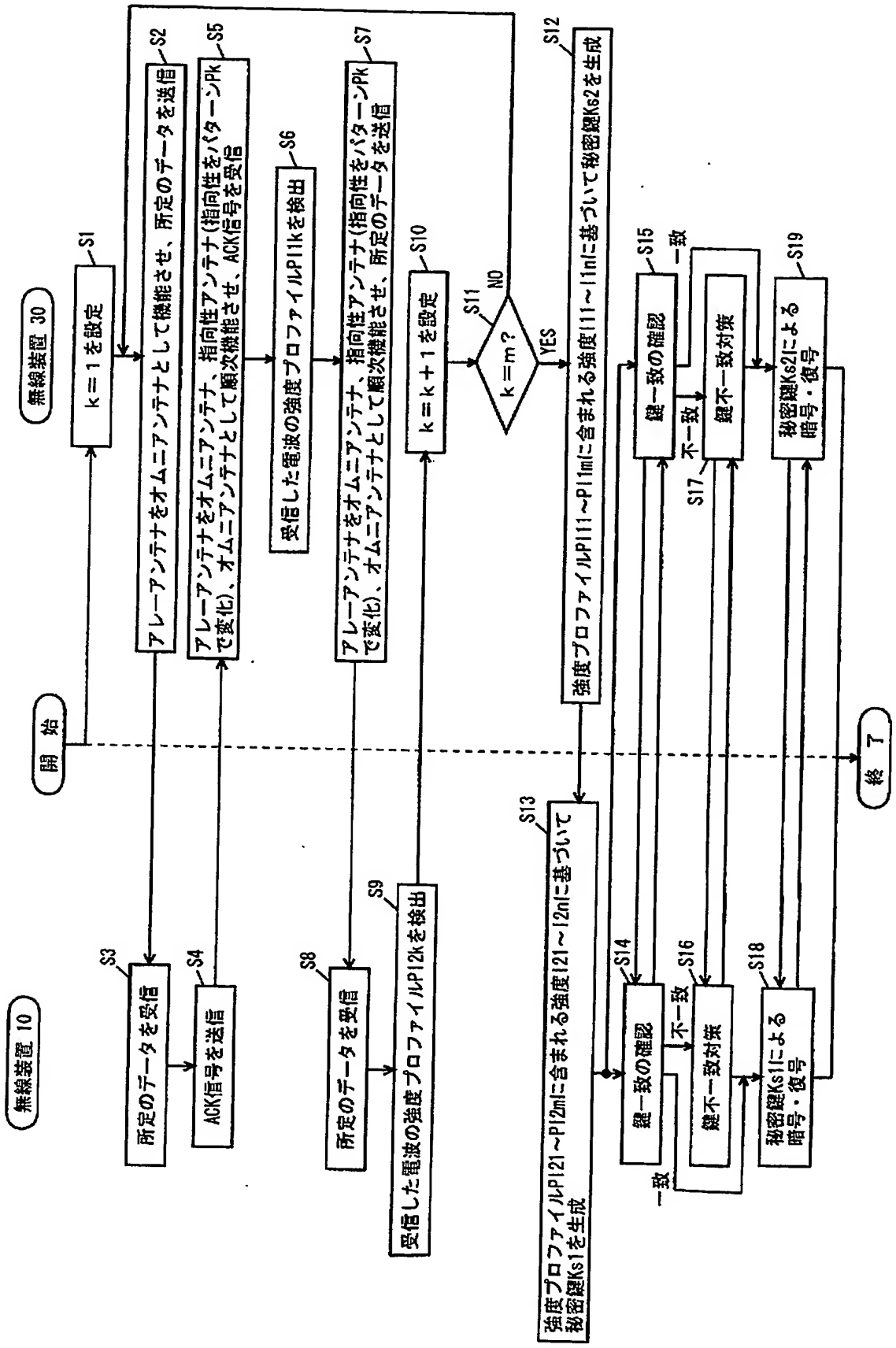
【図１０】


無線装置10
無線装置30
リアクタンス変化パターン(1)
Data
リアクタンス変化パターン(1)
Data
リアクタンス変化パターン(1)
Data

【図１１】


無線装置10
無線装置30
オムニ
パターン
Data
リアクタンス
変化
パターン(1)
Ack
リアクタンス
変化
パターン(1)
Data

【図１２】


無線装置 30
無線装置 10
開　始
終　了
k＝１を設定
S1
アレーアンテナをオムニアンテナとして機能させ、所定のデータを送信
S2
所定のデータを受信
S3
ACK信号を送信
S4
アレーアンテナをオムニアンテナ、指向性アンテナ(指向性をパターンPKで変化)、オムニアンテナとして順次機能させ、ACK信号を受信
S5
受信した電波の強度プロファイルPI1kを検出
S6
アレーアンテナをオムニアンテナ、指向性アンテナ(指向性をパターンPKで変化)、オムニアンテナとして順次機能させ、所定のデータを送信
S7
所定のデータを受信
S8
受信した電波の強度プロファイルPI2kを検出
S9
k＝k＋１を設定
S10
k＝m？
S11
NO
YES
強度プロファイルPI11～PI1mに含まれる強度I11～I1nに基づいて秘密鍵Ks2を生成
S12
強度プロファイルPI21～PI2mに含まれる強度I21～I2nに基づいて秘密鍵Ks1を生成
S13
鍵一致の確認
S14
鍵不一致対策
S16
秘密鍵Ks1による暗号・復号
S18
鍵一致の確認
S15
鍵不一致対策
S17
秘密鍵Ks2による暗号・復号
S19
一致
不一致
一致

【書類名】要約書
【要約】
【課題】　秘密鍵の盗聴を抑制可能な無線通信システムを提供する。
【解決手段】　無線通信システム１００は、無線装置１０，３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０及び３０は、アレーアンテナ２０の指向性を複数個に変えながら所定の通信プロトコル（ＩＥＥＥ８０２．１１ｂ）に従って所定の信号をアンテナ１１及びアレーアンテナ２０を介して相互に送受信する。そして、無線装置１０及び３０は、受信した複数の電波の強度を検出して複数の強度のプロファイルを示す受信信号プロファイルＲＳＳＩ１，２をそれぞれ作成する。無線装置１０及び３０は、それぞれ、受信信号プロファイルＲＳＳＩ１，２の複数の強度を多値化し、その多値化した複数の値をビットパターンとする秘密鍵Ｋｓ１，Ｋｓ２を作成する。
【選択図】　図１

特願２００４－０００５３３

出 願 人 履 歴 情 報

識別番号 [５０３０２７９３１]

１．変更年月日 ２００３年 ４月 ４日
[変更理由] 住所変更
住 所 京都府京都市上京区今出川通烏丸東入玄武町６０１
氏 名 学校法人同志社

特願２００４－０００５３３

出　願　人　履　歴　情　報

識別番号　［３９３０３１５８６］

１．変更年月日　２０００年　３月２７日
［変更理由］　住所変更
住　所　京都府相楽郡精華町光台二丁目２番地２
氏　名　株式会社国際電気通信基礎技術研究所